紀伊國屋数学叢書

28

鈴木 通夫

有限単純群

紀伊國屋書店

はしがき

有限群はすべて単純群を積み重ねて得られる．そこで単純群はどのような群であろうかという質問は，有限群論の根本にある重要な問題であった．過去30年にわたる数多くの人達の努力によって，最近ついに単純群の分類定理が証明された．その定理によれば有限単純群は次の4種類に分類される．すなわち有限単純群は (1) 素数位数の巡回群，(2) 交代群，(3) Lie型の群，および(4) 散在群のいずれかと同形である．

この定理により一般の有限単純群の性質は，上の4種類の各場合にわけて調べることにより解明されることが多い．一例をあげてみよう．有限単純群をGとし，その自己同形群 Aut G をAとおく．この時，外部自己同形群 A/G が可解群になるという主張は古くから Schreier の予想として知られている．分類定理をつかえばGが上の4種類の群のいずれかである時，A/G が可解群になることを確かめればよい．これは巡回群，交代群，Lie 型の群，または散在群の各場合に，それらの群の特別な性質をつかって解決される．このように分類定理から Schreier の予想の正しいことが証明される．(今の時点では，分類定理をつかわずに直接この予想を証明するための手がかりはつかめていない．)

分類定理はこのように単純群の性質を調べるためだけではなく，一般の有限群を調べる上にも今後の発展の基礎となる重要な結果である．しかしその証明は非常に長く，非常に難しいので，分類定理の証明の簡易化をはかること，および分類定理を利用して一般の有限群の性質を解明することが今後の有限群論の二つの中心課題であると思われる．そのためには，まず有限単純群の性質をよく調べることが必要である．

そこで本書では，分類定理にでてくる有限単純群を定義し，それらの群の性質，特にその単純性を証明することを目標とした．巡回群，交代群はよく知られた群であるから，本書では主として Lie 型の群および散在群について述べ

た．Lie 型の群を定義するには Lie 代数の分類をつかう Chevalley の方法に従ったが，そのように定義された群と古典群との関係も詳しく述べた．各散在群の構成について詳しく解説することができなかったのは残念であるが，第4章で各散在群の一応の定義とその単純性の証明を述べた．

本書を読むためには群論の初歩の知識があれば十分であるように努めた．まず第1章には線形代数の復習をかねて，基本的な事柄も含めて線形代数と群論からの準備を解説してある．第2章では他の書との重複をできるだけ少なくするよう努め，一般体上のユニタリ群と，標数2の体上の直交群について詳しく述べた．

第3章では Lie 代数の理論を仮定する．しかしその理論を用いないでも具体的な場合に計算を実行してみれば，理論が示すような群が得られることを確かめることができよう．Lie 代数の理論を学んでから読み返せば更に理解が深まるであろう．

前の章の定理を引用する時，定理 II 4.3 と表わした．これは第2章の定理4.3を意味する．同一の章の定理や命題を引用する時は単に定理1.2または(2.3)などと書き，章の数を表わす記号を省略した．

証明の終りを示すために記号 ▯ を用いた．また同じ記号により定義や注意の終り，証明の略してある定理，命題の終りも表わしてある．

昭和62年6月

鈴　木　通　夫

目　　次

第3章 Lie 型の単純群

第4章 散在単純群

記 号 表

散在単純群の記号は pp. 215—216 の表を参照されたい.

次の記号は慣用のものであるから特にことわらなかった.

$\|G : H\|$	部分群 H の G における指数
$H \lhd G$	H が G の正規部分群であること
$N_G(H)$	部分群 H の正規化群
$C_G(H)$	部分群 H の中心化群
$H \times K$	H と K の直積
$\mathrm{Aut}\ G$	群 G の自己同形全体のつくる群.

第1章 準　　備

§1 序　　説

1. 有限単純群の分類定理 有限群 G が与えられた時 G に含まれる極大正規部分群を N とおけば商群 G/N の正規部分群は自明なもの(単位元だけからなる群 $\{1\}$ およびそれ自身 G/N) だけである．すなわち G/N は**単純群**である．$N=G_1$ とおいて G_1 の極大正規部分群を G_2 とすれば G_1/G_2 はまた単純群となる．このようにして部分群の列

(1.1) $$G=G_0\supset G_1\supset G_2\supset\cdots$$

を G_i が G_{i-1} の極大正規部分群となるようにとれば，商群

$$S_i=G_{i-1}/G_i \qquad (i=1, 2, \cdots)$$

はすべて単純群である．部分群の列 (1.1) は G の**組成列**，単純群 S_i は G の**組成因子**とよばれている．群論のはじめに学ぶ Jordan-Hölder の定理によれば単純群の集合 $\{S_1, S_2, \cdots\}$ は与えられた群 G だけで定まり，組成列の取り方には無関係である．

このように任意の有限群は単純群を積み重ねてできていると考えられる．そこで単純群がどのような群であるか，すなわち単純群の同形類を分類することが有限群論の重要な問題の一つとなる．最近とうとう次の定理が証明されこの問題が解決された．

定理 1.2 有限単純群は次の表のいずれかの群と同形になる．

Ⅰ　素数位数の巡回群，

Ⅱ　交代群，

Ⅲ　Lie 型の単純群，

Ⅳ　26 個の散在単純群．　□

任意の有限群が与えられればその組成列に現われる単純群の集合が定まるので，それらの単純群の性質を用いて任意の有限群のもつ性質を解明することができると期待される．このように定理 1.2 は一般な有限群の構造を調べる鍵と

なる重要な結果で有限群論の今後の発展の基礎となる定理である．しかし今のところ定理1.2の証明は異常に長く，現在(昭和61年夏)でもその証明の全部が印刷され公表されているわけではない．

そこで本書では定理1.2の証明には全く触れず，定理を明確な形で述べることを目標とした．すなわち有限単純群の表に現われる群を定義して，それらが実際に単純群になることを証明するのが本書の目的である．

2. Lie 型の単純群 有限単純群の表に現われる群のうちIおよびIIに属する群はよく知られている群であるからあらためて述べるまでもない．IIIに属する群を定義するには代数群の概念を用いるのが最も簡明であろう．

定義 1.3 代数的閉体の上で定義された単純代数群をGとする．Gの全射自己準同形σによる不変元の全体がつくる集合をG^σとおきG^σが有限集合であると仮定する．この時G^σの組成因子に現われる非可換単純群を**Lie 型の単純群**という． □

この立場にたってLie型の単純群について述べようとすればまず代数的閉体上の単純代数群を分類し，その上で各単純代数群Gの全射自己準同形σのうちG^σが有限群となるものを分類することになる．本書ではあえてこの方向をとらなかった．一つには，この方針に従えば代数群の理論を主として述べなくてはならないということが理由であるが，その他に次の2点がある．代数的閉体上の単純代数群は既約根系というものにより大別される．この時，各根系に対応する単純代数群を構成しなくてはならないが，そのために Lie 代数に対応する Chevalley 群を構成するのが一つの方法である．しかも割合少ない準備の下で群が定義できる利点がある．今一つの点はいわゆる古典群との関係である．群論的にいえばGが例えばD_l型の単純群であるというだけで十分であろう．しかしこの時Gは$2l$次元の線形空間上で定義された指数lの2次形式を不変にする直交群から，交換子群をとり，中心による商群をとるという操作により得られるということも証明しなくてはならないのが有限群論の立場であるように思われる．

そこで本書ではまず古典群を定義し，それからChevalley群，Steinberg群その他の変形を定義することにした．しかしLie型の単純群を理解するためには代数群論の立場から見ることも重要なので本書のあと代数群の教科書および

Steinberg [7] をあわせて勉強されることをおすすめする．

3. 群論からの準備　群 G の２元 x, y が与えられた時，その**交換子**と呼ばれる元 z を

$$z=xyx^{-1}y^{-1}$$

と定義して $z=[x,y]$ と表わす．（この定義は『群論』下で用いている定義と順序が違っている．公式を用いる時など注意する必要がある．）交換子のもつ重要な性質の一つは次の命題である．証明は明らかであろう．

(1.4)　任意の準同形写像 f について

$$f([x,y])=[f(x), f(y)]$$

が成り立つ．特に $g[x,y]g^{-1}=[gxg^{-1}, gyg^{-1}]$ が成り立つ． □

交換子を導入することにより積の順序を変えることができる．すなわち

$$z=[x,y] \Longrightarrow xy=zyx.$$

このように交換子を左に書いて順序が変わるが $xy=yxz'$ と右に交換子を書いて順序を変えることもできる． この場合 $z'=[x^{-1}, y^{-1}]$ である． 群 G の**交換子群** G' は

$$G'=\langle [x,y] \mid x\in G, y\in G\rangle$$

と定義される． ここで記号 $\langle X\rangle$ は部分集合 X から生成される部分群を表わす．交換子群の重要な性質は次の命題である．

(1.5)　群 G の交換子群を G' とおく． G' は G の正規部分群で商群 G/G' は可換群である．逆に G の正規部分群 N に対して商群 G/N が可換群であると仮定すれば，N は交換子群 G' を含む．すなわち交換子群は商群が可換となる正規部分群のうち最小の群である．

証明　(1.4) により交換子の共役元は交換子だから交換子群の生成集合は共役写像により不変となる．したがって G' は G の正規部分群である．

さて $N\triangleleft G$ とし自然準同形 $G\to G/N$ に (1.4) を用いれば

$$[x,y]N=[xN, yN]$$

を得る．よって $N=G'$ ならば左辺は１だから xN と yN とは交換可能である．すなわち G/G' は可換群である． 逆に G/N が可換ならば上式の右辺が１に等しいから $[x,y]\in N$. すなわち任意の交換子が N に含まれるので， G の交換子群 G' は N に含まれる． □

(1.6)　群 G の交換子群を G' とおく．任意の準同形写像 f に対し $f(G')$ は $f(G)$ の交換子群である．

証明　定義と (1.4) から明らかである．□

4. 置換群，群の作用　任意の集合 X の上で定義された**置換**とは X の上で定義された全単射である．すなわち X 上で定義され X の値をとる関数 p について，任意の $y\in X$ に対して $p(x)=y$ をみたす元 $x\in X$ が一意的に存在する時 p を X 上の置換という．いま p, q が共に置換である時，**積** pq を

$$pq(x)=p(q(x))$$

と定義すれば pq はまた X 上の置換となる．(積の定義も『群論』上と順序が違っている．) この積は結合法則 $(pq)r=p(qr)$ をみたすので，X 上の置換の全体は上に定義した積により群をつくる．この群を $\Sigma(X)$ と表わす．$\Sigma(X)$ の部分群を X 上の**置換群**という．

定義 1.7　G を任意の群，X を任意の集合とする．G から $\Sigma(X)$ の中への準同形写像 f が与えられた時，G が f により集合 X の上に**作用する**といい，f を G の**作用**という．□

この定義を敷衍すれば f が G の X 上の作用であるというのは，G の元 g に対して X の置換 $f(g)$ が定まり，任意の $x\in X$ について

$$f(g_1g_2)x=f(g_1)(f(g_2)x) \qquad (g_1, g_2\in G)$$

が成り立つことである．作用 f を省略して $f(g)x$ を gx と書くこともある．この時 G が X に作用しているというのは

$$(g_1g_2)x=g_1(g_2x) \qquad (g_1, g_2\in G)$$

が成り立つことである．

定義 1.8　群 G が集合 X に作用しているとする．X の部分集合 Y が

$$g\in G, y\in Y \Longrightarrow gy\in Y$$

をみたしている時 Y を G **不変な部分集合**という．空集合でない Y が極小の G 不変部分集合である時 Y を G **軌道**という．集合 X 自身が G 軌道である時，G は X に**可移**に作用するという．□

この定義から次の命題が成り立つ．

(1.9) 群 G が集合 X に作用していると仮定する．

(a)　Y を G 軌道とし $y\in Y$ とすれば $Y=\{gy \mid g\in G\}$ が成り立つ．

(b)　X は G 軌道の直和に分解する.

証明　Y を G 軌道とし $y \in Y$ を定める. 定義により任意の $g \in G$ について gy は Y の元である. よって $\{gy\} \subset Y$. ところで任意の $h \in G$ に対し

$$h(gy) = (hg)y$$

が成り立つから $\{gy \mid g \in G\}$ は G 不変である. Y は極小な G 不変部分集合だから (a) が成り立つ.

(a) により二つの G 軌道は一致するか, または共通元を含まない. よって X は互いに共通元を含まない G 軌道の和集合となる. □

群 G が集合 X に作用している時, 任意の元 $x \in X$ について

$$S_G(x) = \{g \mid gx = x\}$$

とおく. 明らかに $S_G(x)$ は G の部分群をつくる. この部分群を x の**安定化群**という. $S_G(x)$ を G_x と表わすこともある.

(1.10)　群 G が有限集合 X 上に可移に作用していると仮定する. X の元を x, その安定化群を H とおけば H の指数は X の元数に等しい. すなわち

$$H = S_G(x) \Longrightarrow |G : H| = |X|.$$

(有限集合 X に含まれる元の数を表わすために記号 $|X|$ を用いる.)

証明　仮定により G は X に可移に作用しているから X は G 軌道となる. よって (1.9) (a) により $X = \{gx\}$ となる. そこで任意に $y \in X$ をとれば $y = gx$ をみたす G の元 g がある. さて

$$gx = hx \Longleftrightarrow h^{-1}gx = x \Longleftrightarrow h^{-1}g \in S_G(x)$$

が成り立つ. よって $y = gx \longmapsto gH$ は X の元と H の剰余類との間の 1 対 1 対応を与える. すなわち (1.10) が成り立つ. □

(1.11)　群 G が集合 X の上に作用しているとする. この時

$$S_G(gx) = gS_G(x)g^{-1}$$

が成り立つ.

証明　$h \in S_G(gx) \Longleftrightarrow hgx = gx \Longleftrightarrow g^{-1}hg \in S_G(x)$. □

§2　線形空間と線形変換群

1. 線形空間の基　　本書で取り扱う線形空間は主として有限次元のものであるが係数体は任意の体としてよい. 特に有限体を係数体とする線形空間が重

要となる．

線形空間 V の係数体を F とおく．V の部分集合 S が与えられた時 F の元を係数とする S の元の一次結合

$$\sum a_i s_i \qquad (a_i \in F, s_i \in S)$$

の全体は V の部分空間をつくる．それを U とおき，S から**生成**される部分空間という．U が S から生成されることを記号

$$U = \langle S \rangle$$

を用いて表わすことにする．U は S を含む最小の部分空間である．特に

$$V = \langle S \rangle \qquad (S \text{ は有限集合})$$

となる時 V は**有限次元**であるという．部分集合 $B = \{v_1, v_2, \cdots, v_n\}$ があって V の任意の元が $\sum a_i v_i$ $(a_i \in F)$ と一意的に表わせる時，B を V の**基**という．表わし方が一意的に定まるから

$$\sum b_i v_i = 0 \ (b_i \in F) \Longrightarrow b_1 = b_2 = \cdots = b_n = 0$$

が成り立つ．すなわち，基の元は一次独立である．逆に V を生成する集合 B の元が一次独立であれば B は V の基である．次の定理が線形空間の基に関する最も重要な命題である．

定理 2.1 有限次元の線形空間は基をもっている．いま

$$\{v_1, \cdots, v_n\}, \quad \{u_1, \cdots, u_m\}$$

が共に空間 V の基であると仮定すれば $n = m$ となり，すべての i について

$$\sigma(v_i) = u_i \qquad (i = 1, 2, \cdots, n)$$

を満足する V の（F に関する）線形写像 σ が唯一つ存在する．空間 V の元 $v_1, v_2, \cdots, v_k$ が F 上一次独立であれば $k \leqq n$ で V の元 $v_{k+1}, \cdots, v_n$ を追加して V の基 $\{v_1, \cdots, v_n\}$ をつくることができる．

証明 $\{v_1, \cdots, v_n\}$ を任意の（V の基とは限らない）集合とする．これらの元の一次結合 $w_1, \cdots, w_m$ が与えられた時 $m > n$ ならば

$$\sum a_i w_i = 0 \qquad (a_i \in F)$$

をみたし，少なくとも一つの係数 a_i が 0 でないような F の元 $a_1, \cdots, a_m$ が存在することを n に関する帰納法により証明しよう．

$n=1$ の場合は $w_1 = av_1, w_2 = bv_1, \cdots$ となる．ここで $w_1 = 0$ ならば $a_1 = 1$, $a_2 = \cdots = 0$ とすればよい．また $w_1 \neq 0$ の場合は

$$a_1=-b,\ a_2=a\neq 0,\ a_3=\cdots=0$$

とすればよい．$n>1$ の場合も $w_m=0$ ならば $a_m=1$ とできる．そこで

$$n>1,\quad m>n,\quad w_m\neq 0$$

と仮定する．この時 $w_m=b_1v_1+\cdots+b_nv_n$ と書けて少なくとも一つの係数は 0 でない．添数をつけかえてもよいから $b_n\neq 0$ と仮定してよい．さて適当に F の元 c_i を選んで $w_i-c_iw_m$ における v_n の係数を 0 にすることができる．そうすれば各 $w_i-c_iw_m$ は $v_1,\cdots,v_{n-1}$ の一次結合となる．したがって帰納法の仮定により F の元 $a_1,\cdots,a_{m-1}$ があって

$$\sum a_i(w_i-c_iw_m)=0$$

が成り立ち，少なくとも一つの係数 a_i は 0 でない．上式の左辺は

$$a_1w_1+\cdots+a_{m-1}w_{m-1}+a_mw_m=0 \qquad (a_m=-\sum a_ic_i)$$

と書き換えられるから始めに述べた命題の成り立つことが証明される．

この命題の特別の場合として $\{v_1,\cdots,v_n\}$ が V の基ならば，V の中の一次独立な元集合は高々 n 個の元しか含んでいないことがわかる．したがって V の部分集合 $\{u_1,\cdots,u_m\}$ も V の基ならば $m=n$ である．

仮定により線形空間 V は有限集合 T から生成されている．そこで T の部分集合のうち V を生成する最小のものを B とおく．B が V の基であることを証明しよう．V の任意の元は B の元の一次結合として表わされるからその表わし方が一意的に定まることを示せばよい．そこで

$$v=\sum a_iv_i=\sum b_iv_i,\quad B=\{v_1,\cdots,v_n\}$$

$(a_i\in F, b_i\in F)$ とおけば $\sum(a_i-b_i)v_i=0$ となる．ここで $a_i\neq b_i$ ならば v_i が $B-\{v_i\}$ に含まれる元の一次結合となり，したがって $B-\{v_i\}$ が V の生成集合となる．これは B が最小であるという仮定に反するからすべての i について $a_i=b_i$ が成り立つ．よって B は V の基である．

さて $\{u_1,\cdots,u_k\}$ が一次独立な元集合であれば $k\leqq n$ であることは前に述べた．そこで $\{u_1,\cdots,u_k\}$ が生成する部分空間を U とおき，$U\neq V$ と仮定しよう．この時 U に含まれぬ V の元を一つとりそれを u_{k+1} とおけば

$$a_1u_1+\cdots+a_ku_k+a_{k+1}u_{k+1}=0 \Longrightarrow a_{k+1}=0$$

が成り立つ．($a_{k+1}\neq 0$ ならば u_{k+1} が $u_1,\cdots,u_k$ の一次結合になる．）すなわち，$u_1,\cdots,u_k,u_{k+1}$ は一次独立で $k+1\leqq n$ となる．この過程を繰り返していけ

ば V の基 $\{u_1, \cdots, u_n\}$ が得られる.

空間 V 上の F 線形写像は基の元での値により定まる. すなわち

$$v=\sum a_i v_i \ (a_i \in F) \Longrightarrow \sigma(v)=\sum a_i \sigma(v_i).$$

したがって $\sigma(v_i)=u_i$ $(i=1, 2, \cdots, n)$ を満足する線形写像 σ は一意的に定まる. 逆に $\sigma(v_i)=u_i$ が与えられれば上式により σ が V 全体で定義される. いま $w=\sum b_i v_i$ とすれば $\alpha v+\beta w=\sum(\alpha a_i+\beta b_i)v_i$ だから

$$\sigma(\alpha v+\beta w)=\alpha\sigma(v)+\beta\sigma(w)$$

が成り立ち σ は V の F 線形写像となる. すなわち σ が一意的に定まる. ▯

有限次元の線形空間 V の基を B とする. B の元数 $n=|B|$ を V の**次元**といい, $\dim V$ と書く. 次元は V だけで定まり基 B の取り方には依存しない (定理 2.1).

系 有限体 F 上 n 次元の線形空間を V とする. F が q 元体ならば

$$|V|=q^n.$$

証明 いま $\{v_1, \cdots, v_n\}$ を V の基とすれば V の元は $\sum a_i v_i$ $(a_i \in F)$ と一意的に書ける. 各係数 a_i は任意に選べるから $|V|=q^n$ となる. ▯

部分空間の次元について次の関係が成り立つ.

(2.2) $$\dim U+\dim W=\dim(U\cap W)+\dim(U+W).$$

ここで $U+W$ は $\{U, W\}$ が生成する部分空間である.

証明 $U\cap W$ の一つの基 $\{v_1, \cdots, v_r\}$ をとりそれを U の基

$$\{v_1, \cdots, v_r, u_1, \cdots, u_s\}$$

に拡張する. また W の基 $\{v_1, \cdots, v_r, w_1, \cdots, w_t\}$ に拡張することもできる. この時 $B=\{v_1, \cdots, v_r, u_1, \cdots, u_s, w_1, \cdots, w_t\}$ とおけば B が $U+W$ の基となることを証明しよう. $U+W$ の元は U の元と W の元との和として表わされるから B が $U+W$ を生成していることは明らかである. そこで

$$\sum a_i v_i+\sum b_j u_j+\sum c_k w_k=0 \qquad (a_i, b_j, c_k \in F)$$

と仮定すれば $\sum b_j u_j=-\sum a_i v_i-\sum c_k w_k \in U\cap W$ を得る. さて $\{v_i\}$ が $U\cap W$ の基だからすべての係数が 0 となり B の元は一次独立である. したがって B は $U+W$ の基となり $\dim(U+W)=r+s+t$ を得る. U, W の次元はそれぞれ $r+s, r+t$ だから (2.2) が成り立つ. ▯

部分空間 U の基 $\{u_1, \cdots, u_k\}$ を V の基 $\{u_1, \cdots, u_k, w_1, \cdots, w_l\}$ に拡張した

とする．この時 $W=\langle w_1, \cdots, w_l \rangle$ とおけば V は

$$V=U \oplus W$$

と直和分解される．この時 W を U の**補部分空間**という．一般に U の補部分空間は沢山あって一意的には定まらない．

(2.3)　線形空間 V の部分空間 U_1 と U_2 が同一次元であると仮定する．この時 U_1, U_2 に共通の補部分空間 W が存在する．すなわち

$$V=U_1 \oplus W=U_2 \oplus W$$

が成り立つような部分空間 W が存在する．

証明　$U_1 \cap U_2$ の一つの基 $\{x_1, \cdots, x_r\}$ を U_1 の基 $\{x_1, \cdots, x_r, y_1, \cdots, y_s\}$ に拡張する．また U_2 の基 $\{x_1, \cdots, x_r, z_1, \cdots, z_t\}$ にも拡張できるが，U_1 と U_2 が同次元だから $s=t$ となる．(2.2) により $\{x_i, y_j, z_k\}$ は U_1+U_2 の基だからそれに V の元 $w_{s+1}, \cdots, w_m$ を加えて V の基をつくることができる．そこで

$$w_i=y_i+z_i \qquad (i=1, 2, \cdots, s)$$

と定義して $W=\langle w_1, \cdots, w_s, w_{s+1}, \cdots, w_m \rangle$ とおく．この W が共通の補部分空間であることを証明しよう．

U_1+W は x_i, y_j, w_k を含むからすべての z_j も含み $U_1+W=V$ となる．そこで $\{x_i, y_j, w_k\}$ が一次独立であることを示そう．さて

$$\sum a_i x_i+\sum b_j y_j+\sum c_k w_k=0 \qquad (a_i, b_j, c_k \in F)$$

と仮定する．$w_1, \cdots, w_s$ にそれぞれ $y_1+z_1, \cdots, y_s+z_s$ を代入して左辺を書き替えれば $\sum a_i x_i+\sum(b_j+c_j)y_j+\sum c_l z_l+\sum' c_k w_k=0$ を得る．ここで最後の和は $k=s+1$ から $k=m$ までの和である．この左辺に現われる V の元は一次独立だからすべての係数が 0 となり $\{x_i, y_j, w_k\}$ は一次独立，したがって直和分解 $V=U_1 \oplus W$ が成り立つ．同様に第二の直和分解 $V=U_2 \oplus W$ が成り立つことも証明される．□

2. 線形変換群　線形空間 V 上の線形写像（または基，次元など）について述べる時は常に V の係数体 F が基礎にあって F に関する線形写像（基，次元など）というべきところであるが，係数体は定まっているので略して単に線形写像ということが多い．

さて V 上の線形写像 f, g が与えられた時 f と g との**積** fg を

(2.4)　$$(fg)(x)=f(g(x))$$

により定義する. f, g と共に fg も V 上の線形写像である.

線形空間 V 上で定義された可逆な線形写像全体の集合を $GL(V)$ と表わす. 明らかに

$$\sigma, \tau \in GL(V) \Longrightarrow \sigma^{-1}, \sigma\tau \in GL(V)$$

が成り立つ. したがって $GL(V)$ は (2.4) で定義された積により群をつくっている. この群を**一般線形変換群**といい, 記号 $GL(V)$ はこの群を表わすものと規約する.

V の一つの基 $\{v_i\}$ を定めると線形写像 f を (n, n) 型の行列により表現できることはよく知られている. すなわち

(2.5) $$f(v_j) = \sum a_{ij} v_i \qquad (j=1, 2, \cdots, n)$$

により (n, n) 型の行列 (a_{ij}) を定義し, $M_f = (a_{ij})$ とおく. M_f を f に**対応する**（または f を**表現する**）行列という. 逆に $M=(a_{ij})$ を任意の (n, n) 型の行列とすれば (2.5) により線形写像 f を定義することができる(定理 2.1 の証明の最終段階参照). この時 M_f の定義により $M=M_f$ となる.

線形写像 f, g に対応する行列をそれぞれ M_f, M_g とおけば

(2.6) $$M_{fg} = M_f M_g$$

の成り立つことが容易に確かめられる. この右辺は行列の積である.

(2.7) 基 $\{v_i\}$ について写像 f を表現する行列を M_f, 別の基 $\{u_i\}$ について f を表現する行列を N_f とおく. 基の変換行列を

$$S=(s_{ij}), \quad v_j = \sum s_{ij} u_i \qquad (j=1, 2, \cdots, n)$$

とおけば $N_f = SM_fS^{-1}$ が成り立つ.

証明 基の逆変換行列を (t_{ij}) とおけば $u_j = \sum t_{ij} v_i$ となる. 行列 M_f および N_f はそれぞれ (2.5) および $f(u_j) = \sum b_{ij} u_i$ により定義されるから

$$\sum b_{ij} u_i = f(u_j) = \sum t_{ij} f(v_i) = \sum t_{ij} a_{ki} v_k$$

が成り立つ. ゆえに $TN_f = M_f T$ を得る. ▯

線形写像 f に対応する行列 M_f は基 $\{v_i\}$ の取り方によって変わるが, 行列式 $\det M_f$ は基の取り方には無関係に f だけで定まる (2.7). そこで任意の線形写像 f に対しその行列式を

$$\det f = \det M_f$$

と定義する. 行列式の性質および(2.6)により写像 $f \longmapsto \det f$ は $GL(V)$ か

ら F の非零元のつくる乗法群（この乗法群を F^* と表わすことにする）の中への準同形写像となる．この写像 det の核を $SL(V)$ と書き**線形変換群**という．今後記号 $SL(V)$ は常に線形変換群を表わすものと規約する．

$$SL(V)=\{\sigma\,|\,\sigma\in GL(V),\ \det\sigma=1\}.$$

写像 det は F^* の任意の元を値にとることができるので次式が成り立つ．

$$\textbf{(2.8)}\qquad GL(V)/SL(V)\cong F^*.$$

空間 V の基 $\{v_1,\cdots,v_n\}$ を定めると V の元を縦ベクトルで表現することができる．すなわち V の元 $v=\sum a_iv_i$ に係数 a_i のつくる縦ベクトル

$$\mathfrak{a}={}^t(a_1,\cdots,a_n)$$

を対応させるのである．線形写像 f の基 $\{v_i\}$ による行列表現を M_f とおけば $f(v)$ に対応する縦ベクトルは $M_f\mathfrak{a}$ である．これは

$$f(v)=\sum a_jf(v_j)=\sum a_ja_{ij}v_i=\sum(\sum a_{ij}a_j)v_i$$

から明らかとなる．

(n,n) 型の行列 M は n 個の縦ベクトルの集まりと見ることができる．このように見れば M_f の第 i 列は $f(v_i)$ に対応する縦ベクトルである．したがって M_f の列ベクトルが一次独立ならば $\{f(v_i)\}$ が一次独立で V の基となる．ゆえに f は可逆で $\det M_f\neq 0$ を得る．これに反し M_f の列ベクトルが一次従属であると仮定すれば（列ベクトルの一つが他の列ベクトルの一次結合となるから）行列式の基本性質により $\det M_f=0$ となる．したがって

$$\textbf{(2.9)}\qquad f\in GL(V)\Longleftrightarrow \det M_f\neq 0$$

が成り立つ．体 F の元を成分とする (n,n) 型の行列でその行列式が 0 でないものの全体は行列の乗法により群をつくる．この群を $GL(n,F)$ と表わす．写像 $\sigma\longmapsto M_\sigma$ は $GL(V)$ から $GL(n,F)$ の中への準同形であるが(2.6)，それは $GL(V)$ と $GL(n,F)$ との間の同形写像である(2.9)．すなわち

$$GL(V)\cong GL(n,F).$$

注意　(2.9)は連立1次方程式の理論における次の定理と同値である．すなわち，連立1次方程式 $\sum a_{ij}x_j=0\ (i=1,2,\cdots,n)$ は $\det(a_{ij})=0$ の時かつその時に限り自明でない解 $(x_1,x_2,\cdots,x_n)$ をもっている．▯

定理 2.10　$SL(V)$ の中心は $\{v\longmapsto\lambda v\}$ $(\lambda\in F^*,\lambda^n=1)$ である．

証明　V の基 $\{v_i\}$ を一つ定めると $\sigma\longmapsto M_\sigma$ により $SL(V)$ は行列式が1

に等しい行列のつくる群と同形になる．そこで $SL(V)$ の中心の元に対応する行列を $\sum a_{ij}e_{ij}$ と行列単位 e_{ij} を用いて表わす．いま $k\neq l$ とすれば $I+e_{kl}$ は $SL(V)$ の元に対応するから

$$(\sum a_{ij}e_{ij})(I+e_{kl})=(I+e_{kl})(\sum a_{ij}e_{ij})$$

を得る．両辺をくらべれば

$$a_{kk}=a_{ll},\qquad a_{ik}=0\quad(i\neq k),\qquad a_{lj}=0\quad(j\neq l)$$

が成り立っている．k,l は任意にとれるから，$SL(V)$ の中心に含まれる元に対応する行列は λI という形をしている．逆にそのような行列は $\lambda^n=1$ ならば $SL(V)$ の中心の元に対応していることは明らかであろう．□

いま $\{v_i\},\{u_i\}$ を V の二つの基とすれば $u_i=\sigma v_i\ (i=1,2,\cdots,n)$ を満足する $GL(V)$ の元 σ が存在する(定理 2.1)．したがって $GL(V)$ は V の零以外の元の集合に可移に作用している．ところで $n\geqq 2$ ならば u_n だけ λu_n に変え，他の u_i を動かさない線形写像 ρ をとれば ρ の行列式は λ で

$$\rho\sigma(v_1)=u_1$$

を満足している．よって $\rho\sigma$ を $SL(V)$ の元にとることができる．

(2.11) 一般線形変換群 $GL(V)$ は $V-\{0\}$ に可移に作用する．V の次元が1より大きければ $SL(V)$ も $V-\{0\}$ に可移に作用する．□

最後に有限体上の $GL(V)$ の位数を計算しよう．

定理 2.12 係数体 F が有限体で $|F|=q, \dim V=n$ とすれば

$$|GL(V)|=(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$
$$|GL(V):SL(V)|=q-1.$$

証明 $\{v_1,\cdots,v_n\}$ を一つの基とすれば任意の $\sigma\in GL(V)$ について

$$\{\sigma v_1,\sigma v_2,\cdots,\sigma v_n\}$$

はまた V の基である．逆に $\{u_1,\cdots,u_n\}$ が V の基であれば $\sigma(v_i)=u_i$ をみたす $GL(V)$ の元 σ が唯一つ存在する(定理 2.1)．したがって $GL(V)$ の位数は V のもつ相異なる基の数に等しい．

基 $\{v_1,\cdots,v_n\}$ を選ぶに当って $v_1,\cdots,v_i$ まですでに選んであると仮定すれば v_{i+1} は $\{v_1,\cdots,v_i\}$ の一次結合にならない任意の元としてよい．ゆえに v_{i+1} は q^n-q^i 通りの取り方がある．よって定理が成り立つ．□

注意 $|GL(n,q)|$ を割る q のベキは丁度 $q^{n(n-1)/2}$ である．□

§3 双対空間

係数体 F 上の n 次元線形空間を V とおく．V から F の中への線形写像全体の集合を V^* とおく．すなわち

$$V^*=\mathrm{Hom}_F(V, F).$$

いま，$f, g\in V^*$ とおけば F の任意の元 α, β について $\alpha f+\beta g$ を

(3.1) $$(\alpha f+\beta g)(v)=\alpha f(v)+\beta g(v)$$

と定義すれば $\alpha f+\beta g$ はまた V^* の元となることが容易に証明される．この加法により V^* は F を係数体とする線形空間となる．この空間を V の**双対空間**という．記号 V^* は常に V の双対空間を表わすものと規約する．

(3.2) V が有限次元ならば $\dim V^*=\dim V$ が成り立つ．

証明 V の基 $\{v_1, \cdots, v_n\}$ を一つ定める．V の元 v を $v=\sum a_iv_i$ と書いた時，v に v_i の係数 a_i を対応させる写像を d_i とおく．すなわち

$$v=\sum a_iv_i \Longrightarrow d_i(v)=a_i$$

とすれば d_i は V^* の元であることがすぐ証明される．そこで $\{d_1, \cdots, d_n\}$ が V^* の基となることを証明しよう．まず V^* の任意の元 f をとれば

$$f=\sum f(v_i)d_i$$

となる．これは $f(v)=\sum a_if(v_i)=\sum f(v_i)d_i(v)$ から明らかである．したがって $\{d_i\}$ は V^* を生成している．さて $\sum b_id_i=0$ $(b_i\in F)$ が成り立つと仮定すれば任意の k について $\sum b_id_i(v_k)=0$ となる．ところで

(*) $$d_i(v_k)=0 \quad (i\neq k), \qquad d_i(v_i)=1$$

だから上式から $b_k=0$ を得る．したがって $\{d_1, \cdots, d_n\}$ は一次独立で V^* の基となる．よって $\dim V^*=\dim V$ が成り立つ．▯

上の証明に出て来た V^* の基 $\{d_1, \cdots, d_n\}$ を V の基 $\{v_1, \cdots, v_n\}$ の**双対基**という．双対基は上の(*)式をみたす V^* の元集合として特長づけられる．

空間 V の元 v は V^* の任意の元 f を $f(v)\in F$ にうつす写像と考えられる．この時，公式 (3.1) は v が V^* から F の中への線形写像であることを示している．この写像を $\varphi(v)$ とおけば φ は V から V^* の双対空間 V^{**} の中への写像である．ところで任意の $f\in V^*$ について

$$\varphi(\alpha v+\beta w)(f)=f(\alpha v+\beta w)=\alpha f(v)+\beta f(w)$$

が成り立つから $\varphi(\alpha v+\beta w)=\alpha\varphi(v)+\beta\varphi(w)$ となる．したがって φ は V から

V^{**} の中への線形写像である．いま $\varphi(v)=0$ ならばすべての $f\in V^*$ について $f(v)=0$，すなわち $v=0$ となる．よって φ は単射で，次元が等しいから φ は V から V^{**} の上への同形写像となる．このように V が有限次元の場合は V を V^* の双対空間と同一視することができる．V の基 $\{v_i\}$ の双対基を $\{d_i\}$ とすれば V^* の基 $\{d_i\}$ の双対基は（V^{**} を V と同一視した時）$\{v_i\}$ と一致する．

定理 3.3　有限次元の線形空間 V の部分空間を U，U^* の任意の元を μ，U に含まれていない V の一つの元を v とする．この時，次の条件を満足する V^* の元 f が存在する：$f(v)=1$ で，さらに U の上で $f=\mu$，すなわち

$$u\in U \Longrightarrow f(u)=\mu(u).$$

証明　U の基 $\{u_1, \cdots, u_m\}$ をとり $u_{m+1}=v$ とおく．さらに $u_{m+2}, \cdots, u_n$ を選んで $\{u_1, \cdots, u_n\}$ が V の基となるようにできる(定理 2.1)．この基 $\{u_1, \cdots, u_n\}$ の双対基を $\{d_1, \cdots, d_n\}$ とし

$$f=\mu(u_1)d_1+\cdots+\mu(u_m)d_m+d_{m+1}$$

とおけば f が求める元である．$u_{m+1}=v$ だから $f(v)=d_{m+1}(v)=1$．また任意の u_i $(i\leqq m)$ について $f(u_i)=\mu(u_i)d_i(u_i)=\mu(u_i)$ となる．したがって f と μ とは U の基 $\{u_1, \cdots, u_m\}$ の各元について一致するから，U 全体で一致し $f=\mu$ となる．▯

線形空間 V から線形空間 W の中への線形写像 φ が与えられた時 φ の双対写像 $\varphi^*: W^*\to V^*$ を次のように定義する．

(3.4)　　$$\varphi^*(f)(v)=f(\varphi(v)) \qquad (f\in W^*, v\in V).$$

任意の元 $f\in W^*$ に対して $\varphi^*(f)$ は V^* の元となり

$$\varphi^*(\alpha f+\beta g)=\alpha\varphi^*(f)+\beta\varphi^*(g) \qquad (f, g\in W^*)$$

が成り立つことも容易に証明される．したがって φ^* は W^* を V^* の中にうつす線形写像である．また次の公式も成り立つ．

$$(\alpha\varphi+\beta\psi)^*=\alpha\varphi^*+\beta\psi^*, \qquad (\varphi\theta)^*=\theta^*\varphi^*.$$

いま V の基 $\{v_1, \cdots, v_n\}$ および W の基 $\{w_1, \cdots, w_m\}$ を定めた時 V から W の中への線形写像 φ に対応する行列 $A=(a_{ij})$ を

$$\varphi(v_j)=\sum a_{ij}w_i \qquad (j=1, 2, \cdots, n)$$

により定める．この時 V^*, W^* にそれぞれ双対基 $\{d_i\}$, $\{e_i\}$ とをれば，双対

写像 φ^* を表現する行列 $B=(b_{ij})$ は

$$\varphi^*(e_j)=\sum b_{ij}d_i \qquad (j=1,2,\cdots,m)$$

と定義される．双対写像の定義 (3.4) により

$$\varphi^*(e_j)(v_k)=e_j(\varphi(v_k))=a_{jk}.$$

一方，$(\sum b_{ij}d_i)(v_k)=b_{kj}$ となる．すなわち B は A の転置行列である．以下行列 A の転置行列を記号

$$^tA$$

を用いて表わす．

§4 双線形形式

係数体が F の線形空間を V とする．体 F の自己同形 θ が与えられた時 V で定義された（θ に関する）**半双線形形式**（単に**形式**ということもある）とは

$$f: V\times V \longrightarrow F$$

つまり V 上で定義され，値を F にとる 2 変数の関数で次の条件

$$\begin{aligned} &f(u_1+u_2, v)=f(u_1, v)+f(u_2, v) \\ \text{(4.1)}\qquad &f(u, v_1+v_2)=f(u, v_1)+f(u, v_2) \\ &f(\alpha u, \beta v)=\alpha\theta(\beta)f(u, v) \qquad (\alpha, \beta\in F) \end{aligned}$$

を満足しているものである．θ が恒等写像の時，f を**双線形形式**という．

本書では形式 f の定義される空間 V は有限次元と仮定する．

任意の $u, v\in V$ について

$$f(u, v)=f(v, u)$$

が成り立つ双線形形式 f を**対称形式**，また任意の $u\in V$ について

$$g(u, u)=0$$

をみたす双線形形式 g を**交代形式**という．体 F の自己同形 θ が $\theta^2=1$ をみたしている時，θ に関する半双線形形式 h について

$$h(u, v)=\theta(h(v, u))$$

がすべての $u, v\in V$ に対し成立する場合 h を **Hermite 形式**（略して単に H 形式）という．この 3 種の形式が重要である．

(4.2) 交代形式 g は次の式をみたす．

$$g(u, v)=-g(v, u) \qquad (u, v\in V).$$

係数体 F の標数が 2 でなければ上式をみたす双線形形式 g は交代形式である．

証明　g が交代形式であると仮定すれば $g(u+v, u+v)=0$ が任意の u, v について成立する．双線形形式の条件式 (4.1) を用いて

$$g(u, u)+g(u, v)+g(v, u)+g(v, v)=0$$

を得る．最初と最後の項は 0 だから $g(u, v)+g(v, u)=0$ が成り立つ．係数体 F の標数が 2 でない時は (4.2) の式において $u=v$ とおけば

$$2g(u, u)=0$$

が得られる．したがって g は交代形式である．□

線形空間 V に一つの基を定めると半双線形形式 f に対応する行列 A_f を次のように定めることができる．いま $\{v_1, \cdots, v_n\}$ を V の基とし

$$A_f=(a_{ij}), \qquad a_{ij}=f(v_i, v_j)$$

とおいて A_f を f に**対応**する行列（または f の**行列表示**）という．さて

$$u=\sum x_i v_i, \quad v=\sum y_i v_i$$

を V の 2 元とすれば $f(u, v)$ の値は (4.1) を用いて

$$f(u, v)=\sum a_{ij} x_i \theta(y_j)$$

と表わされるから f は行列 A_f により完全に定められる．§2 で述べたように V の元 u にその“座標”x_i からなる縦ベクトル $\mathfrak{x}$ を対応させれば

$$f(u, v)={}^t\mathfrak{x} A_f \theta(\mathfrak{y}),$$

ここで $\theta(\mathfrak{y})$ は ${}^t(\theta(y_1), \cdots, \theta(y_n))$ を表わしている．

形式 f の行列表示は V の基を変えれば次のように変換される．いま他の基 $\{u_1, \cdots, u_n\}$ について f に行列 B が対応したとすれば

$$B={}^tTA_f\theta(T).$$

ここで $T=(t_{ij})$ は基の変換式 $u_j=\sum t_{ij} v_i$ の行列である．

定義 4.3　半双線形形式 f が次の条件

$$すべての\ v\in V\ について\ f(u, v)=0 \Longrightarrow u=0$$

を満足している時，形式 f は**非退化**であるという．

定理 4.4　形式 f に関する次の 3 条件は同値である．

(1)　形式 f は非退化である．

(2)　形式 f に対応する行列 A_f が正則である．すなわち $\det A_f \neq 0$.

(3)　すべての $u\in V$ について $f(u, v)=0 \Rightarrow v=0$.

証明 V の基 $\{v_1, \cdots, v_n\}$ を定め f に対応する行列を (a_{ij}) とおく．

(1)⇒(2) A_f が正則でないと仮定すれば連立1次方程式

$$\sum a_{ij}x_i=0 \qquad (j=1, 2, \cdots, n)$$

は自明でない解 $(x_1, \cdots, x_n)$ をもっている．そこで $u=\sum x_i v_i$ とおけば任意の元 $v=\sum y_i v_i$ について $f(u, v)=\sum a_{ij}x_i\theta(y_j)=0$ となる．ところで $u\neq 0$ だから形式 f は退化している．したがって f が非退化ならばその行列表示は正則である．

(2)⇒(3) A_f が正則と仮定する．任意の $u=\sum x_i v_i$ について

$$0=f(u, v)=\sum a_{ij}x_i\theta(y_j) \qquad (v=\sum y_i v_i)$$

が成り立つとすれば，任意の i について（$x_i=1, x_k=0$ $(k\neq i)$ とおき）

$$\sum_j a_{ij}\theta(y_j)=0 \qquad (i=1, 2, \cdots, n)$$

となる．ところで係数のつくる行列式が0でないから，この連立1次方程式には自明な解しかない．すなわち $\theta(y_j)=0$ $(j=1, 2, \cdots, n)$．θ は F の自己同形だから $y_j=0$，したがって $v=0$ を得る．

同様に (3)⇒(2)⇒(1) も証明される．□

(4.5) 線形空間 V で定義された形式を f とおく．任意の $v\in V$ に対し

$$\varphi(v) : u \longmapsto f(u, v)$$

と定義される写像 $\varphi(v)$ は V の双対空間 V^* の元である．この写像 φ は

$$\varphi(v_1+v_2)=\varphi(v_1)+\varphi(v_2), \quad \varphi(\lambda v)=\theta(\lambda)\varphi(v)$$

を満足する．ここで θ は f に同伴する F の自己同形である．（このような写像は V から V^* の中への**半線形写像**と呼ばれている．）特に形式 f が非退化ならば φ は V から V^* の上への全単射となる．この時 φ は V の中で一次独立な集合を V^* の中の一次独立な元集合にうつしている．

証明 前半は明らかであろう．もし f が非退化ならば φ は単射である（定理4.4(3)）．したがって $\{v_1, \cdots, v_k\}$ が一次独立ならば $\{\varphi(v_1), \cdots, \varphi(v_k)\}$ もまた一次独立である．V と V^* は同次元だから φ は全射となる．□

次の定理はしばしば用いられる重要な命題である．

定理 4.6 線形空間 V で定義された形式 f が非退化と仮定する．さらに V の次元を n とする．任意の部分空間 U に対し

$$U^\perp=\{v \mid \text{すべての } u\in U \text{ について } f(u, v)=0\}$$

とおけば $U^\perp$ は V の部分空間でその次元は $n-\dim U$ に等しい．

$$\dim U^\perp = n - \dim U.$$

証明　$U^\perp$ が V の部分空間となることは明らかである．その次元を計算しよう．V の双対空間 V^* の元 g で U の各元 u について $g(u)=0$ をみたすもの全体のつくる集合を U_0 とおく．明らかに U_0 は V^* の部分空間である．

(4.5) によれば形式 f には V から V^* の中への半線形写像 φ が対応している．f が非退化だから φ は全単射である．定義により

$$U^\perp = \varphi^{-1}(U_0)$$

が成り立つから，(4.5) により $\dim U^\perp = \dim U_0$ を得る．

さて $\dim U = m$ とおき $\dim U_0 = n-m$ を証明しよう．$\{v_1, \cdots, v_m\}$ を U の基とすればそれを V の基 $\{v_1, \cdots, v_m, \cdots, v_n\}$ に拡張することができる．そこでその双対基 $\{d_1, \cdots, d_n\}$ をとれば(§3参照)

$$f = \sum a_i d_i \in V^* \Longrightarrow f(v_k) = a_k \quad (k=1, 2, \cdots, n)$$

が成り立つ．したがって

$$f = \sum a_i d_i \in U_0 \Longleftrightarrow a_1 = \cdots = a_m = 0.$$

すなわち $\{d_{m+1}, \cdots, d_n\}$ が U_0 の基となる．よって $\dim U_0 = n-m$ となり定理が成り立つ．□

最後に形式 f の判別式 $\Delta(f)$ を定義しよう．

定義 4.7　基を一つ定め形式 f に対応する行列を A_f とおく．この時

$$\Delta(f) = \det A_f$$

とおき $\Delta(f)$ を f の（定められた基に関する）**判別式**という．

注意　この定義では基の取り方によって判別式 $\Delta(f)$ の値が変わる．□

§5　内積空間と古典群

線形空間 V で定義された半双線形形式 f が条件

(5.1)　　$$f(u, v) = 0 \Longleftrightarrow f(v, u) = 0$$

を満足している時 $f(u, v)$ を V の元 u, v の**内積**という．本書では内積の定義された空間を**内積空間**ということにする．つまり内積空間とは V と f との組 (V, f) である．(§4の規約により内積空間は有限次元である．)

二つの内積空間 (V, f) と (V', f') が与えられた時 V から V' の中への線形

写像σがVとV'との間の同形写像であって，さらに

$$f'(\sigma u, \sigma v)=f(u, v)$$

がすべての$u, v\in V$について成り立つ時σを(V, f)から(V', f')の上への**等長写像**という．内積空間(V, f)のそれ自身の上への等長写像の全体を

$$\mathrm{Aut}(V, f)$$

と表わす．$\mathrm{Aut}(V, f)$は$GL(V)$の部分集合であるが明らかに$GL(V)$の部分群をつくっている．

以下本書で考察する内積空間(V, f)ではfは非退化かつfは対称，交代，または Hermite 形式のいずれかである．おのおのの場合に応じて$\mathrm{Aut}(V,f)$をそれぞれ**直交群**，**斜交群**，または**ユニタリ群**と呼び，上の3種類の群に線形変換群を加えたものを**古典群**と総称する．これらの群は一般に単純ではないが行列式の値が1の元のつくる部分群をその中心で割った商群は一般に単純群になる．直交群の場合は行列式の値を1にするだけでは不充分で，交換子群をとらなくてはならない．この様にして**古典単純群**が得られる．これらの事実を証明するのが第2章，第3章の主な目的である．

内積空間を調べるに当って次の概念が重要となる．

定義 5.2　内積空間(V, f)を考える．任意の部分空間UについてfのU上への制限をgとおけば内積空間(U, g)が得られる．部分空間U, Wがあって線形空間としてVはUとWとの直和となり，その上

$$u\in U, w\in W \Longrightarrow f(u, w)=0$$

が成り立つ時Vは部分空間UとWとの**直交和**に分解するという．▯

この時$V=U\perp W$と表わすこともあるが，単にVは直交和$U\oplus W$に分解すると表わすことが多い．(記号$\oplus$は線形空間としての直和を表わす.)

(5.3)　内積空間(V, f)において形式fは非退化であると仮定する．部分空間Uが与えられた時$V=U\oplus W$と直交和に分解するための条件は形式fのU上への制限gが(U上の)非退化形式となることである．この時WはUにより一意的に定まる．すなわち$W=U^{\perp}$が成り立つ．

証明　$W=U^{\perp}$とおく．fが非退化だから定理4.6により

$$\dim W=n-\dim U \qquad (n=\dim V)$$

が成り立つ．さてU上へのfの制限gが非退化であるための条件は

$$U \cap U^{\perp} = \{0\}$$

である．したがって g が非退化ならば $V=U\oplus W$ と直交和に分解する．そして逆も成り立つ．明らかに $W=U^{\perp}$ は U により一意的に定まる．□

最後に $GL(V)$ の元が $\mathrm{Aut}(V,f)$ に属するための条件を求めておこう．

定理 5.4 内積空間 (V,f) に一つの基 B を定める．この時 f に対応する行列を $A=A_f$ とおく．$GL(V)$ の元 σ に対応する行列を M_σ とすれば

$$\sigma\in \mathrm{Aut}(V,f) \Longleftrightarrow {}^tM_\sigma A\theta(M_\sigma)=A$$

が成り立つ．ここで θ は f に同伴している係数体の自己同形である．

証明 $B=\{v_1, v_2, \cdots, v_n\}$ とおけば $A=(a_{ij})$ $(a_{ij}=f(v_i, v_j))$,

$$\sigma v_j=\sum b_{ij}v_i, \quad M_\sigma=(b_{ij})$$

が成り立つ．さて $\sigma\in \mathrm{Aut}(V,f)$ は $f(\sigma v_i, \sigma v_j)=f(v_i, v_j)$ と同値で

$$a_{ij}=\sum b_{ki}\theta(b_{lj})a_{kl}, \quad \text{すなわち} \quad A={}^tM_\sigma A\theta(M_\sigma)$$

が成り立つ時，かつその時に限り $\sigma\in \mathrm{Aut}(V,f)$ となる．□

系 1 内積空間 (V,f) において形式 f は非退化と仮定する．この時

$$\sigma\in \mathrm{Aut}(V,f) \Longrightarrow (\det\sigma)\theta(\det\sigma)=1.$$

証明 定理 5.4 で用いた記号をそのまま用いる．f が非退化だから

$$\det A\neq 0$$

となる(定理 4.4)．したがって $(\det M_\sigma)\,\theta(\det M_\sigma)=1$ を得る．□

系 2 直交群の元 σ に対して $\det\sigma=\pm1$ が成り立つ．

証明 $\theta=1$ だから系 1 より系 2 が証明される．□

注意 斜交群の場合は $\det\sigma=1$ となる(定理 II 5.4)．直交群は行列式の値が -1 の元も含んでいる．□

内積空間として 3 種類の特別な空間だけを特に取り上げる理由は次の定理が成り立つことによる．

定理 5.5 内積空間 (V,f) において f は非退化，$\dim V>1$ と仮定する．この時，形式 f は対称形式であるか，交代形式であるかまたは $f=ch$．ここで c は F の元，h は Hermite 形式となる．したがって $\mathrm{Aut}(V,f)$ は直交群，斜交群またはユニタリ群となる．□

証明は永尾 [4] pp. 161–163 を参照されたい．また形式が非退化と限らない場合には次の定理が成り立つ．

(5.6)　内積空間を (V, f) とする．いま部分空間 V_0 を

$$V_0=\{v \mid \text{すべての } u\in V \text{ について } f(u, v)=0\}$$

と定義して $\overline{V}=V/V_0$ とおく．さらに $\bar{f}(v+V_0)=f(v)$ とおけば $\bar{f}$ は $\overline{V}$ で定義された半双線形写像で $(\overline{V}, \bar{f})$ は非退化内積空間となる．そして

$$G=\mathrm{Aut}(V, f)$$

は正規部分群 N を含み，N は可換群，さらに

$$G/N\cong GL(V_0)\times \mathrm{Aut}(\overline{V}, \bar{f})$$

が成り立つ．N は $\overline{V}$ から V_0 の中への F 線形写像全体のつくる加法群に同形で G は N と $GL(V_0)\times\mathrm{Aut}(\overline{V}, \bar{f})$ との半直積となる．その作用は

$$((\sigma, \rho)f)(v)=\sigma(f(\rho^{-1}v)) \qquad (v\in \overline{V})$$

で与えられる．ここで $\sigma\in GL(V_0), \rho\in\mathrm{Aut}(\overline{V}, \bar{f}), f\in\mathrm{Hom}_F(\overline{V}, V_0)$.　□

証明には定理 5.4 を用いればよいがここでは省略する．

第2章　古　典　群

§1　交代群の単純性

n 個の文字 $\{1,2,\cdots,n\}$ の上の偶置換の全体のつくる群を n 文字の**交代群**といい A_n で表わす．定義から直ちに次の命題が得られる．

(1.1)　交代群 A_n は二つの互換の積で表わされる元から生成される．　□

さて置換 σ が二つの互換の積であるとしよう．σ の二つの因子が共通の文字を動かしていれば $\sigma=(ab)(bc)$ と書けるから $\sigma=(abc)$ となり σ は3巡回置換である．σ の因子が動かす文字が異なっていれば σ は $(2,2)$ 型の置換である．A_n に含まれている3巡回置換全体のつくる集合を T_n とおく．

(1.2)　$n\geqq 3$ ならば交代群 A_n は T_n から生成される．

証明　a,b,c,d が異なる4文字を表わしていると仮定すれば

$$(ab)(cd)=(abc)(bcd)$$

となる．したがって (1.1) および上述の注意により (1.2) が成り立つ．　□

(1.3)　$n\geqq 5$ ならば T_n は A_n の共役類となる．

証明　(abc) および (efg) を二つの3巡回置換とする．いま

$$a\longrightarrow e,\quad b\longrightarrow f,\quad c\longrightarrow g$$

をみたす置換を σ とおけば $\sigma(abc)\sigma^{-1}=(efg)$ となる．$\sigma\notin A_n$ と仮定すれば σ は奇置換である．$n\geqq 5$ と仮定したから $\{e,f,g\}$ 以外に2元 $\{h,j\}$ をとり $\tau=(hj)$ とおく．そうすれば $\tau\sigma$ は偶置換で

$$\tau\sigma(abc)\sigma^{-1}\tau^{-1}=(efg)$$

となる．したがって (abc) と (efg) とは A_n の中で共役である．　□

注意　(123)と(132) とは A_4 の中では共役にならない．　□

定理 1.4　$n\geqq 5$ ならば交代群 A_n は単純群である．

証明　交代群 A_n の正規部分群を N とおく．まず N が3巡回置換を含んでいれば $N=A_n$ となることを証明しよう．N に含まれている3巡回置換を θ とおき，A_n の任意の3巡回置換を θ' とする．(1.3) により θ' は θ と A_n の中

で共役であるから $\theta'=\sigma\theta\sigma^{-1}$ をみたす $\sigma\in A_n$ がある．したがって

$$\theta'=\sigma\theta\sigma^{-1}\in\sigma N\sigma^{-1}=N,$$

すなわち N はすべての3巡回置換を含んでいる．よって $N=A_n$ (1.2).

以下 $N\neq\{1\}$ と仮定して N が3巡回置換を含むことを証明しよう．N の非単位元 ρ をとり ρ は3巡回置換ではないと仮定する．ρ の型を $(r_1,\cdots)$ とし $r_1\geqq 4$ の場合は長さ r_1 の巡回置換を一つ取り上げて

$$\rho=(ab\cdots cd)\cdots$$

とおく．$r_1\leqq 3$ ならば ρ は長さ1以上の巡回置換を少なくとも二つ含むから

$$\rho=(ab\cdots)(cd\cdots)\cdots$$

とおく．いずれの場合も a,b,c,d は互いに相異なる4文字を表わす．さて

$$\theta=(acd),\quad \gamma=[\rho,\theta]=\rho\theta\rho^{-1}\theta^{-1}$$

とおけば $\rho\theta\rho^{-1}=(bd*)$ となるから $\gamma\neq 1$ を得る．ところで $\rho\in N$ だから $\theta\rho\theta^{-1}\in N$, よって $\gamma\in N$ が成り立つ．一方，γ は二つの3巡回置換の積で高々5文字を動かしている．もし γ が3巡回置換ならば N は3巡回置換を含む．また γ が3巡回置換でなければ γ は5巡回置換であるかまたは(2, 2)型である．そこで

$$\gamma=(xyzwt)\ \text{または}\ \gamma=(xy)(zw),\quad \tau=(xyt)$$

とおけば交換子 $[\gamma,\tau]$ は N に含まれる3巡回置換となる．よって N は3巡回置換を含み前述のように $N=A_n$. よって A_n は単純群である．∎

§2 射影線形変換群の単純性

この節では任意の係数体 F 上の有限次空間 V をとる．そして $SL(V)$ をその中心で割った商群が二つの例外の場合を除けば単純群となることを証明しよう．証明に当って幾何の概念が重要な働きをする．空間 V の次元を n とおく．部分空間 H の次元が $n-1$ の時 H を V の**超平面**という．超平面に関する移換という概念を定義しよう．

定義 2.1 H を V の超平面とする．$GL(V)$ の元 $\tau\neq 1$ が次の条件

(1) すべての $v\in V$ について $\tau(v)-v\in H$, および

(2) すべての $u\in H$ について $\tau(u)=u$

を満足している時 τ を (H に関する) **移換**という．

(2.2)　H を V の超平面とし V の双対空間 V^* の元 μ で $\ker\mu=H$ を満足するものを一つ定める．H の任意の元 a をとり線形写像 $\tau(\mu,a)$ を

$$\tau(\mu,a):v\longmapsto v+\mu(v)a$$

と定義する．もし $a\neq0$ ならば $\tau(\mu,a)$ は H に関する移換である．逆に H に関する移換は $\tau(\mu,a)$ $(a\neq0)$ と表わすことができる．また

$$\tau(\mu,a)\tau(\mu,b)=\tau(\mu,a+b)\qquad(a,b\in H)$$

が成り立つ．

証明　$\tau(\mu,a)$ が移換のみたすべき条件(1)，(2)を満足していることは明らかである．もし $a\neq0$ ならば $\tau(\mu,a)\neq1$ だから $\tau(\mu,a)$ は移換である．

H に関する移換の一つを τ とする．適当に $a\in H$ を選べば $\tau=\tau(\mu,a)$ と表わすことができることを示そう．V の元 v で $\mu(v)=1$ をみたすものをとり $a=\tau(v)-v$ とおく．移換の条件(1)により $a\in H$ となる．$v\notin H$ だから V の任意の元 x は $x=\lambda v+u$ $(\lambda\in F, u\in H)$ と一意的に書くことができる．そこで $\mu(x)=\lambda\mu(v)+\mu(u)=\lambda$ が成り立つから

$$\tau(x)=\lambda\tau(v)+\tau(u)=\lambda(v+a)+u=x+\mu(x)a$$

となる．すなわち $\tau=\tau(\mu,a)$ を得る．

最後の式が成り立つことは明らかであろう．□

(2.3)　超平面 H を定め H に関する移換の全体に単位元 1 を加えた集合を $T(H)$ とおく．$T(H)$ は $SL(V)$ の部分群で加法群 H と同形である．

証明　(2.2) により $T(H)$ の元は $\tau(\mu,a)$ $(a\in H)$ と書くことができる．また (2.2) の最後の式により $T(H)$ は群をつくり

$$\tau(\mu,a)\longmapsto a$$

が $T(H)$ から H の上への同形写像を与える．□

定理 2.4　移換は $SL(V)$ の元である．また，移換はすべて $GL(V)$ の中で共役となる．すなわち τ,τ' を二つの移換とすれば，$\tau'=\sigma\tau\sigma^{-1}$ を満足する元 $\sigma\in GL(V)$ がある．$n\geqq3$ ならば $\sigma\in SL(V)$ とすることができる．超平面 H を定めれば任意の移換 τ は $SL(V)$ の中で H に関する移換と共役になる．すなわち $\sigma\tau\sigma^{-1}\in T(H)$ をみたす $\sigma\in SL(V)$ が存在する．

証明　超平面 H に関する移換を τ とする．(2.2)の証明中に定めたように元 v,a をとる．さて a は H の元で 0 ではないから $v_2=a$ からはじめて H の基

$\{v_2, v_3, \cdots, v_n\}$ をとることができる．これに $v_1=v$ を加えれば V の基となる．この基に関して線形写像 τ を表現する行列は左上の隅に

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

があってあとは単位行列に一致する．よって τ は $SL(V)$ の元である．

任意の移換を τ' とする．この場合 V の基 $\{u_1, \cdots, u_n\}$ を適当にとれば τ' がやはり上述の行列により表現される．そこで $\sigma(v_i)=u_i$ $(1 \leqq i \leqq n)$ をみたす $GL(V)$ の元 σ をとれば

$$\sigma\tau\sigma^{-1}(u_1)=u_1+u_2, \qquad \sigma\tau\sigma^{-1}(u_i)=u_i \quad (i \geqq 2)$$

が成り立つから $\sigma\tau\sigma^{-1}=\tau'$ となる．したがって τ' は τ と共役である．

$n \geqq 3$ の場合は u_n の代りに λu_n $(\lambda \neq 0)$ を選んでも τ' は同じ行列によって表現される．この時，基の変換行列の行列式はもとの行列式に λ を掛けたものだから適当に λ を選んで $\sigma \in SL(V)$ とすることができる．

$n=2$ の場合 u_2 の代りに λu_2 を選んで変換行列の行列式を 1 にすると移換 τ' を表現する行列が変わって

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

となる．この場合 τ' は τ と共役にならないかも知れないが基 $\{v_1, v_2\}$ に関して上の行列で表現される $T(H)$ の元 τ_1 が τ' と共役になる．すなわち任意の移換は $SL(V)$ の元により $T(H)$ の元と共役になる． ▯

定理 2.5 $n \geqq 3$ ならば任意の移換は $SL(V)$ の元の交換子として表わされる．すなわち，移換 τ は $\tau=[\sigma, \rho]$ $(\sigma, \rho \in SL(V))$ と書ける．

$n=2$ の場合も $|F| \geqq 4$ ならば同じ命題が成り立つ．

証明 超平面 H と群 $T(H)$ を考える．$n \geqq 3$ ならば $\dim H \geqq 2$ だから $|H|$ は少なくとも 4 である．(2.3) により $T(H) \cong H$ だから $T(H)$ は移換 α, β $(\alpha \neq \beta)$ を含む．したがって $\gamma=\alpha\beta^{-1}$ は移換である．$\beta=\delta\alpha\delta^{-1}$ $(\delta \in SL(V))$ となるから ($n \geqq 3$ と仮定している)

$$\gamma=\alpha\beta^{-1}=\alpha\delta\alpha^{-1}\delta^{-1}=[\alpha, \delta]$$

を得る．任意の移換 τ は γ と共役だから τ も交換子の形に書ける．

$n=2$ の場合 V の基 $\{v_1, v_2\}$ を $v_1 \in H$ をみたす様に選べば $T(H)$ は

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

という形の行列で表現される元からなる部分群である．そこで $s \in F^{*}$ とし

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}^{-1}=\begin{pmatrix} 1 & t(1-s^2) \\ 0 & 1 \end{pmatrix}$$

を得る．$|F| \geqq 4$ ならば $s \neq 0, s^2 \neq 1$ をみたす F の元 s がある．したがって $T(H)$ の元はすべて交換子の形に書ける．移換は $SL(V)$ の中で $T(H)$ の元と共役だから任意の移換が $SL(V)$ の元の交換子となる．▯

定理 2.6 移換全体のつくる集合を T とおけば $SL(V)=\langle T \rangle$．すなわち T が生成する部分群は $SL(V)$ と一致する．

証明 $G=\langle T \rangle$ とおく．$G \neq SL(V)$ と仮定して矛盾を導こう．σ による不変元の全体を $I(\sigma)$ と表わす．すなわち $I(\sigma)=\{v \in V \mid \sigma(v)=v\}$．さて G に含まれていない $SL(V)$ の元のうち $I(\sigma)$ が極大になるものを一つ定め，それを σ とおく．そして $U=I(\sigma)$, $U(v)=\langle U, v \rangle$ と定義する．

(a) 任意の元 $v \in V$ について $\sigma(v) \in U(v)$ が成り立つことを証明しよう．そこで或る元 $x \in V$ について $\sigma(x) \notin U(x)$ と仮定し $\sigma(x)-x=a$ とおく．もし $x \in U(a)$ ならば $\sigma(x)=x+a \in U(a)=U(x)$ となり仮定に反する．したがって $x \notin U(a)$ となる．よって $U(a)$ 上で $0, x$ での値が 1 の V^{*} の元 μ がある（定理 I 3.3）．いま $\tau=\tau(\mu, a)$ とおけば τ は移換で（(2.2)参照）

$$\tau(x)=x+\mu(x)a=\sigma(x), \qquad \tau(u)=u=\sigma(u) \quad (u \in U)$$

が成り立つ．したがって $I(\tau^{-1}\sigma) \supseteq U(x) \supsetneqq U$ となる．σ と共に $\tau^{-1}\sigma \notin G$ だから，これは $U=I(\sigma)$ を極大にとったことに矛盾する．

(b) (a) で証明したことは任意の $v \in V$ について $\sigma(U(v))=U(v)$ が成り立つことと同値である．つぎに U が V の超平面であることを証明しよう．明らかに $\sigma \neq 1$ だから U は V の真の部分空間である．そこで U を含む超平面の一つを H とする．H に関する任意の移換 τ がすべての $x \in V$ について

$$\tau(x)-x \in U$$

を満足していることを示そう．H に関する移換の定義から $\tau(x)-x \in H$ を得る．もし $x \in H$ ならば $\tau(x)=x$ だから上の関係式は明らかに成り立つ．そこで $x \notin H$ と仮定しよう．元 $\tau\sigma$ は G に含まれずかつ U の各元を不変にするか

ら $U(x)=\tau\sigma(U(x))=\tau(U(x))$ が成り立つ ((b) 当初の注意). さて $\tau(x)\in U(x)$ だから $\tau(x)-x\in U(x)\cap H=U$ ($x\notin H$ だから), すなわち任意の $x\in V$ について $\tau(x)-x\in U$ が成り立つ. ところで (2.3) によれば, τ が $T(H)$ を動くとき $\tau(x)-x$ の形の元は H を生成する. したがって U は H と一致する.

(c)　明らかに σ は V/U に線形写像 $\bar{\sigma}$ を引きおこす. σ は U 上で恒等写像と一致するから $\det\bar{\sigma}=\det\sigma=1$ が成り立つ. (b) により V/U は1次元だから任意の $v\in V$ について $\sigma(v)-v\in U$ となる. したがって σ が超平面 U に関する移換となり, $\sigma\notin G$ という仮説に矛盾する. ▯

系　$n\geqq 3$ または $|F|\geqq 4$ ならば $SL(V)$ はその交換子群と一致する.

証明　定理2.5により任意の移換は交換子となる. よって定理2.6により系が成り立つ. ▯

定理 2.7　(n,n) 型の単位行列を I とおく. また (i,j) 成分だけが1で他の成分がすべて0の (n,n) 型行列を e_{ij} とおく. 行列群 $SL(n,F)$ は

$$\{I+te_{ij}\mid t\in F, i\neq j\}$$

から生成される.

証明　$G=\langle I+te_{ij}\ (t\in F, i\neq j)\rangle$ とおき $G=SL(n, F)$ となることを証明しよう. $SL(n, F)$ は n 次元の縦ベクトル全体がつくる線形空間 V の上に自然に作用している. V の自然な基を $\{x_1, \cdots, x_n\}$ とおく. この基により $SL(n, F)$ は $SL(V)$ と同一視できるから G がすべての移換を含むことを証明すればよい.

(a)　いま $x_2, \cdots, x_n$ が生成する超平面を H_0 とおく. H_0 に関する移換は

$$I+\sum\alpha_i e_{i1}=\prod(I+\alpha_i e_{i1})$$

と表わされるから G の元である. すなわち G は H_0 に関する移換をすべて含んでいる.

(b)　つぎに G が V の超平面の集合に可移に作用していることを証明しよう. そのため V の双対空間 V^* の上への $SL(n, F)$ の作用を考える. V の自然な基に双対な V^* の基を $\{d_1, \cdots, d_n\}$ とすれば $SL(n, F)$ の元 M の V^* の上への作用は M の転置行列によって与えられる. したがって G は $V^*-\{0\}$ に可移に作用している. さて任意に超平面 H をとれば $H=\ker\mu$ をみたす V^* の元 $\mu\neq 0$ がある. そこで ${}^t\sigma(\mu)=d_1$ をみたす G の元 σ をとれば

$$\sigma(H_0)=H$$

が成り立つ．よって G は V の超平面の集合に可移に作用している．

(c) 任意の移換 τ をとり，τ が超平面 H に関する移換であるとする．(b) により $\sigma(H)=H_0$ をみたす G の元 σ がある．したがって $\sigma\tau\sigma^{-1}$ は H_0 に関する移換である．(a) により $\sigma\tau\sigma^{-1}\in G$，すなわち $\tau\in G$ を得る． ▯

$SL(V)$ の構造を調べるに当って $SL(V)$ が自然に作用する集合と，その上の作用を調べることが重要になる．$SL(V)$ は $V-\{0\}$ に作用しているがこの作用より V の部分空間のつくる集合の上への作用の方が自然で重要である．

線形空間 V の部分空間全体からなる集合を V 上の**射影空間**といい $\mathcal{P}(V)$ と表わす．V の1次元部分空間に対応する $\mathcal{P}(V)$ の元を**点**という．$\mathcal{P}(V)$ の点 P をとれば P は V の1次元部分空間だからその生成元を x とする．この時 x を点 P の**代表元**という．x と共に αx $(\alpha\in F^{\#})$ も P の代表元である．

定理 2.8 $SL(V)$ は射影空間 $\mathcal{P}(V)$ の点集合の上に2重可移に作用する．

証明 $\mathcal{P}(V)$ の2点 P, Q $(P\neq Q)$ を代表する V の元 u, v をとれば u と v とは一次独立である．したがって $\{u, v\}$ を最初の2元とする基 B がある．さて V の基 $\{x_1, \cdots, x_n\}$ を一つ定めておけば B を $\{x_1, \cdots, x_n\}$ に移す元 $\sigma\in GL(V)$ がある．σ は $\{u, v\}$ を $\{x_1, x_2\}$ に移している．元 x_i が代表する $\mathcal{P}(V)$ の点を P_i とおけば $\sigma(P)=P_1, \sigma(Q)=P_2$ となる．P の代表元として αu がとれるから $\det\sigma=1$ にすることができる．すなわち $SL(V)$ は2重可移に作用している． ▯

(2.9) $SL(V)$ が $\mathcal{P}(V)$ の点集合の上に引きおこす置換群は

$$PSL(V)=SL(V)/Z$$

である．ここで Z は $SL(V)$ の中心で $v\longmapsto\lambda v$ $(\lambda^n=1)$ という写像の全体である．

証明 いま $\mathcal{P}(V)$ の各点を動かさない元の全体を Z とおけば $SL(V)$ が引きおこす置換群は $SL(V)/Z$ と表わされる．V の基 $\{x_1, \cdots, x_n\}$ を一つ定めれば Z の元 ζ について $\zeta(x_i)=\alpha_i x_i$ $(\alpha_i\in F, i=1, \cdots, n)$ が成り立つだけでなく $x_i+x_j\to\alpha(x_i+x_i)$ $(i\neq j)$ も成り立つ．よって $\alpha(x_i+x_j)=\alpha_i x_i+\alpha_j x_j$ より $\alpha_i=\alpha=\alpha_j$ を得る．したがって

$$\zeta(v)=\lambda v \qquad (v\in V)$$

となりλはvに無関係な定数である．$\zeta\in SL(V)$ より $\lambda^n=1$ が成り立つ．ζの形からζは $SL(V)$ の中心に含まれていることがわかる．

逆にζが $SL(V)$ の中心の元ならば $\zeta(v)=\lambda v$ となることは前に述べた(定理 I 2.10)．よって (2.9) が成り立つ．□

定義 2.10　$PSL(V)$ を**射影線形変換群**という．

定理 2.11　$PSL(V)$ は次の2例外を除けば単純群である．例外は $n=2$ で $|F|\leqq 3$ の場合である．例外の場合 $PSL(V)$ は可解群で単純ではない．

この定理を証明するために必要となる群論の補題を二つ証明する．まず次の概念を解説しよう．集合X上に可移に作用している群GにおいてXの元xの安定化群がGの極大部分群である時Gは**原始的**に作用するという．

(2.12)　群Gが2重可移に作用していれば原始的に作用する．

証明　集合Xの上にGが2重可移に作用していると仮定する．Xの1元aの安定化群をG_aとおく．いまG_aに含まれていない元 σ, τ をとり

$$\sigma\in\langle G_a, \tau\rangle$$

を証明しよう．そこで $\sigma(a)=b, \tau(a)=c$ とおけば $b\neq a, c\neq a$ である．Gは2重可移だから $\rho(a)=a, \rho(b)=c$ をみたす元 $\rho\in G$ がある．定義により $\rho\in G_a$. また $\tau^{-1}\rho\sigma(a)=\tau^{-1}\rho(b)=a$ より $\tau^{-1}\rho\sigma\in G_a$. すなわち $\sigma\in\langle G_a, \tau\rangle$ が成り立つ．σは任意だから $\langle G_a, \tau\rangle=G$ が成り立つ．したがってG_aはGの極大部分群で，Gは原始的である．□

(2.13)　Gは集合X上の置換群としX上に可移に作用していると仮定する．Gの正規部分群を N, $a\in X$ の安定化群をG_aとおく．もし $N\subset G_a$ ならば $N=\{1\}$ となる．

証明　Xの任意の元bをとれば（Gの作用が可移だから）$\sigma(a)=b$ を満足するGの元σがある．したがって $G_b=G_{\sigma(a)}=\sigma G_a\sigma^{-1}\supset\sigma N\sigma^{-1}=N$ を得る(I (1.11)参照)．ところでbは任意だからNの元はXのすべての元を不変にする．すなわち $N=\{1\}$ が成り立つ．□

次に岩沢の定理を証明しよう．

定理 2.14　集合Xの上の可移置換群Gが次の3条件を満足していると仮定する．

(1)　GはXに原始的に作用している．

(2) G の交換子群 G' は G と一致する.

(3) X の元 a の安定化群 G_a は可解な正規部分群 Q を含み，G は Q の共役部分群全体により生成される.

以上の仮定の下で G は単純群である.

証明 G の正規部分群を N とし $N\neq\{1\}$ と仮定する. (2.13) により N は G_a の部分群ではない. したがって NG_a は G_a より大きい部分群となる. 仮定(1)により G_a は極大部分群だから

$$G=NG_a$$

を得る. 部分群 NQ を考えよう. Q は G_a の正規部分群だから G_a は N および Q を正規化する. すなわち $NQ\lhd\langle N, G_a\rangle=NG_a=G$ が成り立つ. 条件(3)により G は Q の共役部分群で生成されるから

$$G=NQ$$

が成り立つ. したがって $\overline{G}=G/N$ とおけば同形定理により

$$\overline{G}=G/N=NQ/N\cong Q/Q\cap N$$

となる. (2)により $G=G'$ だから $\overline{G}$ の交換子群 $\overline{G}'$ は $\overline{G}$ に一致する(I (1.6)). 一方, Q は可解群だから $\overline{G}\cong Q/Q\cap N$ も可解群である. 交換子群と一致する可解群は $\{1\}$ に限るから $\overline{G}=\{1\}$, すなわち $N=G$ が成り立つ. したがって G は単純群である. □

定理 2.11 の証明 $G=PSL(V)$ を射影空間の点集合の上の置換群と考えれば((2.9)参照) 定理 2.8 により 2 重可移に作用している. したがって(2.12)により作用は原始的で G は条件(1)を満足する.

定理 2.6 系により二つの例外の場合を除けば $SL(V)$ はその交換子群と一致する. G は $SL(V)$ の準同形像だから $G=G'$ となり条件(2)も成り立つ.

最後に条件(3)も成り立つことを証明しよう. $SL(V)$ を行列の群と同一視して $\mathcal{P}(V)$ の 1 点（例えば x_1 が代表する点）の安定化群 G_a を考えれば G_a は

$$\begin{pmatrix} \alpha & * \\ 0 & A \end{pmatrix}$$

という形の行列（ここで $\det A=\alpha^{-1}$）全体のつくる行列群 H を $SL(V)$ の中心 Z で割った商群に一致する. この行列群 H の各元を上の形に書いて

$$\theta : \begin{pmatrix} \alpha & * \\ 0 & A \end{pmatrix} \longmapsto A$$

を考えれば θ は準同形写像である．明らかに $\ker\theta$ は

$$\begin{pmatrix} 1 & * \\ 0 & I \end{pmatrix} \qquad (I\text{は }(n-1, n-1)\text{ 型の単位行列})$$

からなる群である．さて $K=\ker\theta$ とおけば $K \lhd H$ が成り立つ．そこで

$$Q=KZ/Z$$

とおけば $H/Z=G_a$ だから $Q \lhd G_a$ となる．K の元の形から K は可換群となり Q も可換群である．明らかに K は移換を含むから K の共役部分群全体は $SL(V)$ を生成する(定理 2.4, 2.6)．したがって Q の共役部分群全体の集合は $PSL(V)$ を生成し条件(3)が成り立つ．

このように例外の場合を除けば $G=PSL(V)$ は定理 2.14 の仮定をみたしているから G は単純群となる．

例外の場合．$|F|=2$ ならば $|G|=6$ で $PSL(V)$ は 3 次の対称群と同形である．一方 $|F|=3$ ならば $PSL(V)$ の位数は 12 で 4 次の交代群と同形になる．いずれの場合も $PSL(V)$ は可解群で単純ではない．▯

注意　定理 2.11 の証明は岩沢先生の方法によるものを述べた．交代群の場合の証明の方針に従って証明することもできる．これについてはたとえば『群論』上 p. 75 を参照されたい．▯

最後に次の定理を証明しておこう．

定理 2.15　定理 2.11 の例外の場合を除けば $SL(V)$ の真の正規部分群は中心に含まれている．

証明　$G=SL(V)$ とおき G の中心を Z とする．さて G の正規部分群 N が中心に含まれていないと仮定しよう．この時 $NZ \lhd G$ だから

$$G/Z \rhd LZ/Z \neq \{1\}$$

となる．ところで定理 2.11 により G/Z は単純群であるから $G=NZ$ を得る．したがって同形定理により $G/N \cong Z/N\cap Z$ が成り立つ．Z は G の中心だから可換群である．上の同形対応により G/N が可換群となる．したがって N は G の交換子群を含んでいる．ところで定理 2.6 系により $G=G'$ が成り立つから $N=G$ となり定理が証明される．▯

§3 内積空間の分類

この節では内積空間 (V, f) は**非退化**と仮定する(I §5参照). さらに f が対称形式である場合には係数体 F の標数は2でないと仮定する.

定義 3.1 内積空間 (V, f) の元 x が $f(x,x)=0$ をみたす時 x は**等方的**という. 二つの元の組 $\{x,y\}$ が次の条件

$$f(x,x)=f(y,y)=0, \quad f(x,y)=1$$

をみたしている時 $\{x,y\}$ を**双曲型**の組という. 双曲型の組 $\{x,y\}$ が生成する平面 $\langle x,y\rangle$ を**双曲型平面**という. 一般に双曲型平面の直交和となっている部分空間を**双曲型の部分空間**という.

注意 組 $\{x,y\}$ が双曲型かどうかはもち論与えられた形式 f による. 正確にいえば組 $\{x,y\}$ が形式 f に関して双曲型であるというべきであるが, 以下 f は定まっていると認めて一々ことわらないことにする. 双曲型の組 $\{x,y\}$ の2元 x,y は一次独立である. したがって x,y が生成する部分空間は2次元である. さて双曲型平面 P をとれば, P は双曲型の組 $\{a,b\}$ により生成されている. そこで写像 $\sigma:\lambda x+\mu y\longmapsto\lambda a+\mu b$ を考えれば σ は $\langle x,y\rangle$ から P の上への等長写像を与える. すなわち双曲型平面はすべて同型である. 同様に双曲型の部分空間が同次元の時それらは同形である. ▯

定理 3.2 内積空間 (V, f) において f が非退化交代形式とすれば, V は双曲型である. 特に $\dim V=n$ は偶数で (V, f) は次元により一意的に定まる.

証明 任意の元 $a\neq0$ に対して $f(a,u)\neq0$ をみたす $u\in V$ がある(f が非退化). そこで $\lambda f(a,u)=1$ をみたす F の元 λ をとり $b=\lambda u$ とおく.

$$f(a,b)=1, \quad f(a,a)=f(b,b)=0$$

だから $P=\langle a,b\rangle$ は双曲型平面となり, 直交和分解 (I (5.3)参照)

$$V=P\oplus P^{\perp}$$

が成り立つ. さて $V_1=P^{\perp}$ とおき f の V_1 上への制限を f_1 とすれば f_1 は V_1 で定義された非退化交代形式となる. 次元に関する帰納法により定理が証明される. ▯

対称形式とH形式を調べるために次の補題が必要である.

(3.3) 内積空間 (V,f) において形式 f は対称またはH形式と仮定する. 部分空間 U の各元が等方的ならば f の U 上への制限は自明, すなわち

$$f(x,y)=0 \qquad (x,y\in U).$$

証明 仮りに $f(x_0,y_0)\neq0$ となる $x_0,y_0\in U$ があったとしよう. U の各元

が等方的だから任意の $u, v \in U$ について

$$f(u, v) = -f(v, u)$$

が成り立つ(I (4.2)の証明参照)．そこで形式 f に同伴する係数体 F の自己同形を θ とすれば，F の任意の元 λ に対して

$$\begin{aligned}\lambda f(x_0, y_0) &= f(\lambda x_0, y_0) = -f(y_0, \lambda x_0) \\ &= -\theta(\lambda) f(y_0, x_0) = \theta(\lambda) f(x_0, y_0)\end{aligned}$$

が成り立つ．$f(x_0, y_0) \neq 0$ より $\theta(\lambda) = \lambda$ を得る．よって $\theta = 1$，すなわち f は対称形式である．そこで

$$f(x_0, y_0) = f(y_0, x_0) = -f(x_0, y_0)$$

が成り立つ．対称形式の場合，係数体の標数は2でないと規約したからこれは矛盾である．よって (3.3) が成り立つ．□

定理 3.4　内積空間 (V, f) において f は非退化な対称形式または H 形式とする．この時 V は1次元空間の直交和となる．

証明　補題3.3により非等方的元 u がある．そこで $L = \langle u \rangle$ とおけば

$$V = L \oplus L^{\perp}$$

と直交和に分解する．定理3.2の証明と同様に帰納法が適用される．□

定義 3.5　内積空間 (V, f) の基 $\{u_1, \cdots, u_n\}$ が次の条件

$$f(u_i, u_j) = 0 \qquad (i \neq j)$$

をみたす時 $\{u_1, \cdots, u_n\}$ を V の**直交基**という．さらに $f(u_i, u_i) = 1$ がすべての i について成り立つならば**正規直交基**という．□

係数体が有限体の場合をさらに詳しく調べよう．まず f が H 形式の場合を考える．この時，同伴自己同形 θ の不変体を F_0 とおけばガロア理論により F は F_0 の2次の拡大体である $(\theta^2 = 1)$．よって

$$|F_0| = q$$

とおけば F は q^2 元体で任意の $\lambda \in F$ に対して $\theta(\lambda) = \lambda^q$ が成り立つ．任意の元 $u \in V$ をとればエルミット条件から

$$f(u, u) = f(u, u)^q \in F_0$$

を得る．ところで有限体では次の補題が成り立つ．

(3.6)　上の記号を用いれば F_0 の元 a は λ^{1+q} と表わせる．

証明　乗法群 $F^{\#}$ は位数 $q^2 - 1$ の巡回群である．そこで写像

$$\nu : \alpha \longmapsto \alpha^{1+q}$$

を考えれば ν は $F^{\#}$ の自己準同形でその核の位数は $q+1$ である．したがって ν の像の位数は $q-1$ となり $\mathrm{Im}\ \nu=(F_0)^{\#}$ を得る．ところで $a=0$ の場合は自明だから F_0 の各元は λ^{1+q} と表わすことができる．▯

定理 3.7　非退化 H 形式による有限体上の内積空間 (V, f) には正規直交基をとることができる．したがって (V, f) は次元 $\dim V$ により一意的に定まる．

証明　定理 3.4 により V は直交基 $\{u_1, \cdots, u_n\}$ をもっている．前に注意したように $f(u_i, u_i)\in F_0$ だからおのおのの i について

$$\lambda_i^{1+q} f(u_i, u_i)=1$$

をみたす $\lambda_i\in F$ が存在する (3.6)．そこで $v_i=\lambda_i u_i$ とおけば $\{v_1, v_2, \cdots, v_n\}$ は V の正規直交基である．▯

次に対称形式の場合を考えよう．この場合 $|F|=q$ は奇数である．

(3.8)　有限体 F の任意の元 α に対し $\alpha=\xi^2+\eta^2$ をみたす元の組 (ξ, η) が存在する．

証明　自乗の形に表わされる元の集合を S とおく．F の標数が 2 の場合には $S=F$ となるから命題は明らかに成り立つ．$|F|=q$ が奇数の場合，乗法群 $F^{\#}$ の元の自乗 $(F^{\#})^2$ は位数 $(q-1)/2$ の部分群をつくる．したがって

$$|S|=((q-1)/2)+1=(q+1)/2$$

となる．これから S は加法群 F の部分群ではないことがわかる．(もし部分群ならば $|S|$ は $|F|$ の約数でなければならない．) よって

$$\beta=(\xi_0)^2+(\eta_0)^2\notin S$$

をみたす元の組 (ξ_0, η_0) がある．さて命題は $\alpha\in S$ の時明らかに成り立つ．そこで $\alpha\notin S$ と仮定すれば $\alpha\in(F^{\#})^2\beta$ だから $\alpha=\lambda^2\beta$．よって α も二つの自乗元の和となる．▯

定理 3.9　奇標数の有限体 F の上で非退化対称形式をもつ内積空間 (V, f) の同形類はどの次元でも二つ存在する．すなわち (V, f) の同形類は次元 n と形式 f の判別式 $\Delta(f)$ により定まる．

$$(V, f)\cong(U, g) \Longleftrightarrow \dim V=\dim U,\ \Delta(f)/\Delta(g)\in(F^{\#})^2.$$

証明　いま f も g も対称形式であって $(V, f)\cong(U, g)$ ならば U と V の次元

が等しいことは明らかである．任意に基を定めて f,g に対応する行列をそれぞれ M_f, M_g とすれば定義により

$$\varDelta(f)=\det M_f,\quad \varDelta(g)=\det M_g$$

である．一方，等長写像 $U\to V$ による U の基の像を V の基にとれば，f に対応する行列が M_g と一致する．したがって I §4 により

$${}^tTM_gT=M_f$$

となる．よって $d^2\varDelta(g)=\varDelta(f)$ $(d=\det T)$ を得る．

逆を証明するために f の標準形を求めよう．$(F^*)^2$ に含まれていない元 $\gamma\neq 0$ を一つ定めておく．定理 3.4 により直交基 $\{u_1, \cdots, u_n\}$ がとれる．

$$f(u_i, u_i)=\gamma_i \qquad (i=1, 2, \cdots, n)$$

とおけば u_i を λu_i に変えても直交基であることに変わりはないから各 i について $\gamma_i=1$ または $\gamma_i=\gamma$ と仮定することができる．ここで実は

$$\gamma_1=\gamma_2=\cdots=\gamma_{n-1}=1$$

をみたす直交基がとれることを証明しよう．そこで $\gamma_i=\gamma_j=\gamma$ と仮定する．この時 $v=\alpha u_i+\beta u_j$ とおけば $f(v, v)=(\alpha^2+\beta^2)\gamma$ となる．(3.8) により適当に α, β を選んで $(\alpha^2+\beta^2)\gamma=1$ とできる．よって $f(v, v)=1$, すなわち u_i の代りに v を直交基の一員に選べば $\{\gamma_i\}$ の中に現われる γ の数をへらすことができる．すなわち $\{\gamma_i\}$ の中に γ が高々一つしか現われないような直交基がとれる．さて $\gamma_1=\cdots=\gamma_{n-1}$ とすれば

$$\varDelta(f)=\gamma_n$$

であるから次元と判別式で同形類が決定される． ▯

注意 次元 n が奇数の場合，正規直交基をもつ対称内積空間を (V, f) とする．この時 $\varDelta(f)=1$ である．上の証明で用いたように γ を定め，形式 γf を考える．これも非退化対称形式だが内積空間 $(V, \gamma f)$ の判別式は

$$\varDelta(\gamma f)=\gamma^n.$$

仮定により n は奇数だから $(V,\gamma f)$ と (V, f) とは同形でない．ところで

$$\mathrm{Aut}(V,f)=\mathrm{Aut}(V,\gamma f).$$

したがって奇数次元の直交群は次元により一意的に定まる．偶数次元の場合，非同形な内積空間から非同形な直交群が得られる．このことは後で述べよう． ▯

2 次元の場合をさらに調べてみよう．まず次の補題を証明する．

(3.10) (V, f) を 2 次元の非退化内積空間とする．V の元 u, v が

$$f(u, u)=0, \quad f(u, v)\neq 0$$

を満足していれば (V, f) は双曲型平面である．

証明 v の代りに αv を考えてもよいから $f(u, v)=1$ と仮定することができる．f が交代形式ならば $\{u, v\}$ は双曲型の組だから V は双曲型平面である．そこで f は対称形式または H 形式と仮定する．

さて $w=\lambda u+v$ $(\lambda\in F)$ とおけば $f(u, w)=1$ および

$$f(w, w)=\lambda+\theta(\lambda)+a \qquad (a=f(v, v))$$

が成り立つ．ここで θ は形式 f に同伴している F の自己同形である．f が対称形式ならば F の標数は 2 でないから $\lambda=-a/2$ とおけば $\{u, w\}$ は双曲型の組となる．明らかに $\{u, w\}$ が生成する平面は V と一致する．一方 f が H 形式ならば $a=f(v, v)$ は θ の不変体 F_0 の元である．この時，次の補題が成り立つ．

不変体 F_0 の元 b が与えられれば $\mu+\theta(\mu)=b$ をみたす F の元 μ がある．

(**証明** $\theta\neq 1$ だから $\theta(x)\neq -x$ をみたす F の元 x が存在する．そこで

$$c=x+\theta(x)$$

とおけば c は F_0 の元で $c\neq 0$ となる．よって $\mu=xbc^{-1}$ とおけば

$$\mu+\theta(\mu)=b.)$$

したがって適当に λ を選んで $f(w, w)=0$ とすることができる．前と同様に V が双曲型平面となる．▯

系 非退化対称形式をもつ 2 次元の内積空間は双曲型平面（判別式は -1）であるかまたは直交基 $\{x, y\}$ をもち $f(x, x)=1$, $f(y, y)=-\gamma$ (γ は非自乗元) をみたす平面 W（判別式は $-\gamma$）のいずれかと同形になる．W は 0 以外に等方的な元を含まない．▯

定理 3.11 奇標数の有限体の上で非退化対称形式をもつ内積空間 (V, f) は

$$V=P_1\oplus\cdots\oplus P_r\oplus R$$

と直交和に分解する．ここで $P_1, \cdots, P_r$ は双曲型平面，$\dim R\leqq 2$，かつ R は 0 以外の等方的元を含まない．もし $\dim R=2$ ならば R は上にあげた平面 W と同形である．

証明 次元 $n=2m+1$ が奇数とする．$P_1, \cdots, P_m$ を双曲型平面とし

$$P_1\oplus\cdots\oplus P_m\oplus R, \quad R=Fu$$

の判別式を計算すれば $\Delta(f)=(-1)^m f(u,u)$ となる．したがって $f(u,u)$ の値により $\Delta(f)$ は平方元にも非平方元にもなる．$n=2m$ が偶数ならば（定理 3.9）

$$P_1 \oplus \cdots \oplus P_m \quad と \quad P_1 \oplus \cdots \oplus P_{m-1} \oplus W$$

とは非同形で任意の対称内積空間はこのいずれかと同形になる．□

§4 Witt の定理

内積空間を考えるにあたって最も基本的な定理がこの節で述べる Witt の定理である．まず次の定義から始めよう．

定義 4.1 内積空間 (V, f) の部分空間 U に対しその**根基** rad U を

$$\mathrm{rad}\, U = U \cap U^{\perp}$$

と定義する．部分空間 U が rad $U=\{0\}$ をみたす時，U を**非等方的**といい，rad $U \neq \{0\}$ の時，**等方的**という．特に rad $U=U$ が成り立つ時，U を**全等方的**という．□

定義から明らかであるが任意の U に対して rad U は全等方的である．

(4.2) 内積空間 (V, f) の部分空間 U が非等方的であるための条件は内積 f の U への制限が U 上で非退化なことである．もし f が非退化で U が非等方的ならば直交和分解 $V=U \oplus U^{\perp}$ が成り立つ．

証明 部分空間 U の元 x が rad U に属するための条件は $f(u,x)=0$ が U の任意の元 u について成り立つことだから (4.2) の前半が成り立つ．後半は I (5.3) で証明されている．□

基本定理の証明に次の命題が必要である．

(4.3) 内積空間 (V, f) において形式 f は非退化と仮定する．V の部分空間 U に対し rad U の基 $\{u_1, \cdots, u_r\}$ および rad U の U における補部分空間 W が与えられていると仮定する．この時，次の性質をもつ元の組

$$\{v_1, \cdots, v_r\}$$

が存在する．すべての i について $\{u_i, v_i\}$ は双曲型の組となる．いま

$$P_i = \langle u_i, v_i \rangle, \quad U_0 = \langle U, v_1, \cdots, v_r \rangle$$

とおけば $U_0 = P_1 \oplus P_2 \oplus \cdots \oplus P_r \oplus W$ と直交和に分解し rad $U_0=\{0\}$．

証明 命題を r に関する帰納法で証明しよう．仮定により直交和分解

$$U = W \oplus \langle u_1, u_2, \cdots, u_r \rangle$$

が成り立つ．もし $r=0$ ならば結果は自明であるから $r>0$ と仮定し

$$U_1=W\oplus\langle u_1,\cdots,u_{r-1}\rangle$$

とおく．この時 U_1 は u_r を含まないから $U^{\perp}$ は $(U_1)^{\perp}$ の真の部分空間となる．そこで $(U_1)^{\perp}-U^{\perp}$ の元 v をとれば $f(u_r,v)\neq 0$．元 u_r は等方的だから (3.10) により $\langle u_r,v\rangle$ は双曲型平面である．よって適当に $\langle u_r,v\rangle$ の元 v_r をとり $\{u_r,v_r\}$ が双曲型の組となるようにできる．さて

$$P_r=\langle u_r,v_r\rangle,\quad V_1=(P_r)^{\perp}$$

とおけば $V=P_r\oplus V_1$ および $U_1\subset V_1$ が成り立つ．いま形式 f の V_1 上への制限を f_1 とおけば f_1 は非退化である．この時

$$V_1, f_1, U_1, W\quad \text{および}\quad \{u_1,\cdots,u_{r-1}\}$$

が帰納法の仮定をみたしていることが容易に証明される．よって帰納法の仮定により $\{v_1,\cdots,v_{r-1}\}$ が存在し $P_i=\langle u_i,v_i\rangle$ について直交和分解

$$U_2=P_1\oplus\cdots\oplus P_{r-1}\oplus W$$

が成り立つ．さらに $U_2\subset V_1$, $U_2\cap U_2{}^{\perp}\cap V_1=\{0\}$ となる．明らかに

$$U_0=U_2\oplus P_r=P_1\oplus\cdots\oplus P_r\oplus W$$

は直交和である．さて $x\in \mathrm{rad}\,U_0$ とすれば $x\in(P_r)^{\perp}$ だから

$$x\in U_0\cap V_1=U_2$$

となる．よって $x\in U_2\cap U_2{}^{\perp}\cap V_1=\{0\}$，すなわち $\mathrm{rad}\,U_0=\{0\}$．　□

さて Witt の定理は次のように述べられる．

定理 4.4 内積空間 (V,f) と (V_1,f_1) は共に非退化で互いに同形であると仮定する．この時 V の任意の部分空間を U とすれば U から V_1 の中への等長写像は V から V_1 の上への等長写像に拡張できる．

まず証明に必要な補題を二つ証明する．

(4.5) 内積空間 (V,f) の中に部分空間 U, W および等長写像

$$\sigma: U\longrightarrow V,\quad \tau: W\longrightarrow V$$

が与えられ，$U\cap W=\{0\}$，$\sigma(U)\cap\tau(W)=\{0\}$，さらに

$$f(\sigma u,\tau w)=f(u,w),\quad f(\tau w,\sigma u)=f(w,u)$$

がすべての $u\in U, w\in W$ について成り立っていると仮定する．この時

$$\rho: u+w\longmapsto \sigma u+\tau w$$

は $U+W$ から V の中への等長写像である．

証明 条件 $U\cap W=\{0\}=\sigma(U)\cap\tau(W)$ により ρ は単射となる．さて

$$f(\sigma u+\tau w, \sigma x+\tau y) \qquad (u, x\in U, w, y\in W)$$

を展開すれば，仮定により各項から σ, τ が落せるので

$$f(\sigma u+\tau w, \sigma x+\tau y)=f(u+w, x+y),$$

すなわち ρ は等長写像である．▯

(4.6) 内積空間 (V, f) は非退化と仮定する．さらに部分空間 U から V の中への等長写像 σ が与えられているとする．この時 U を含む非等方的部分空間 U_0 があって，σ は U_0 から V の中への等長写像に拡張できる．

証明 いま $\mathrm{rad}\,U$ の基 $\{u_1, \cdots, u_r\}$ をとり $U=W\oplus\mathrm{rad}\,U$ と分解する．(4.3) により V の元 $\{v_1, \cdots, v_r\}$ があって $\{u_i, v_i\}$ は双曲型の組，

$$U_0=P_1\oplus\cdots\oplus P_r\oplus W \qquad (P_i=\langle u_i, v_i\rangle)$$

は直交和，さらに U_0 は非等方的となる．そこで

$$X=\sigma(U), \qquad Y=\sigma(W), \qquad x_i=\sigma(u_i) \quad (i=1, 2, \cdots, r)$$

とおけば，σ は等長写像だから $\{x_1, x_2, \cdots, x_r\}$ は $\mathrm{rad}\,X$ の基となり

$$X=Y\oplus\mathrm{rad}\,X$$

が成り立つ．また (4.3) により V の元 $\{y_1, \cdots, y_r\}$ があって，すべての i について $\{x_i, y_i\}$ は双曲型の組となる．さて $Q_i=\langle x_i, y_i\rangle$ とおけば

$$X_0=Q_1\oplus\cdots\oplus Q_r\oplus Y$$

は直交和である．そこで $\sigma_0: U_0\to X_0$ を U 上では σ に等しく

$$\sigma_0(v_i)=y_i \qquad (i=1, 2, \cdots, r)$$

と定義すれば σ_0 が U_0 から X_0 の上への等長写像に拡張できることは明らかである．▯

定理 4.7 非退化な内積空間 (V, f) の部分空間 U をとる．この時 U から V の中への等長写像は (V, f) の自己同形に拡張できる．

証明 まず等長写像 $\sigma: U\to V$ が U の1元 x を $y\neq x$ に動かすが，ある超平面 W の各元を固定する場合を考える．この時 $D=\{\sigma u-u\}$ $(u\in U)$ とおけば D は $\sigma x-x$ が生成する1次元の部分空間である．さて

$$f(\sigma u-u, \sigma v)=f(u, v)-f(u, \sigma v)=f(u, v-\sigma v)$$

が任意の $u, v\in U$ について成り立つ．したがって $W\subset D^\perp$ となる．

場合を分け，まず $x\notin D^\perp$ の場合を考える．上式で $u=v=x$ とおいてみれ

ば $y=\sigma x$ も $D^\perp$ に含まれていないことがわかる．そこで

$$\text{恒等写像}: D^\perp \longrightarrow D^\perp, \quad \sigma: Fx \longrightarrow Fy$$

に (4.5) が適用できることを示そう．さて，$D^\perp$ の任意の元 z は

$$f(u, z)=f(\sigma u, z), \quad f(z, u)=f(z, \sigma u) \qquad (u \in U)$$

をみたすから (4.5) が適用される．この場合 $W=U\cap D^\perp$ だから拡張された等長写像が σ の拡張となっていることは明らかであろう．また $V=Kx+D^\perp$ だから σ は (V, f) の自己同形に拡張される．

次に $x\in D^\perp$ の場合を考える．今度は $y=\sigma x$ も $D^\perp$ に含まれるから U および σU は $D^\perp$ の同次元の部分空間である．よって I (2.3) により $D^\perp$ の中で共通の補部分空間 X をもっている．$\sigma: U\to\sigma U$ と恒等写像 $X\to X$ に対して (4.5) が適用され，σ は $U+X=D^\perp$ の等長写像 τ に拡張できる．ところで $\sigma x, x$ 共に $D^\perp$ に含まれるから $D\subset D^\perp$，すなわち $D^\perp$ は等方的．したがって (4.6) により τ は更に大きい次元の非等方的部分空間に拡張される．この場合 $D^\perp$ は V の超平面だから結局 σ は V 上に拡張される．

一般の場合は $\dim U$ に関する帰納法により次のように証明される．U の超平面 W を定めれば σ の W への制限は帰納法の仮定により (V, f) の自己同形 τ_1 に拡張される．そこで $\tau_1^{-1}\sigma$ を考えればこれは W の恒等写像を与えている．もし τ_1 が σ の拡張であれば証明終り．もし τ_1 が σ の拡張でなければ $\tau_1^{-1}\sigma$ は始めに述べたように (V, f) の自己同形 τ_2 に拡張される．したがって自己同形 $\tau_1\tau_2$ は σ の拡張である． □

定理 4.4 の証明 仮定により $(V, f)\cong(V_1, f_1)$ だから V から V_1 の中への等長写像 θ がある．U から V_1 の中への等長写像を σ とすれば $\theta^{-1}\sigma$ は U から V の中への等長写像であるから定理 4.7 により (V, f) の自己同形 τ に拡張できる．明らかに $\theta\tau$ は V から V_1 の上への等長写像で U の上では $\theta(\theta^{-1}\sigma)=\sigma$ と一致する．すなわち定理 4.4 が成り立つ． □

系 内積空間 (V, f) は非退化と仮定する．極大な全等方的部分空間 U_1 と U_2 に対して $U_2=\tau(U_1)$ をみたす $\tau\in\mathrm{Aut}(V, f)$ がある．特に

$$\dim U_1=\dim U_2.$$

証明 まず $\dim U_1\leqq\dim U_2$ と仮定する．この時 U_1 から U_2 の中への単射線形写像 σ がある．ところで U_1 も U_2 も全等方的であるから σ は等長写像

である．よって Witt の定理により σ は (V, f) の自己同形 τ に拡張される．すなわち $\tau(U_1)=\sigma(U_1)\subset U_2$ が成り立つ．したがって $U_1\subset\tau^{-1}(U_2)$ を得る．τ^{-1} も等長写像であるから $\tau^{-1}(U_2)$ は全等方的．ところで U_1 は極大の全等方的部分空間だから $U_1=\tau^{-1}(U_2)$ となる．

もし $\dim U_1\geqq\dim U_2$ であっても同様に証明される．▯

定義 4.8 内積空間 (V, f) が非退化の時，極大な全等方的部分空間の次元を形式 f の**指数**という．▯

定理 4.7 の系により指数は (V, f) により定まり極大全等方的部分空間の取り方には無関係である．

定理 4.9 非退化内積空間 (V, f) の指数を ν，$\dim V=n$ とおけば

$$2\nu\leqq n$$

が成り立つ．この時 $V=P_1\oplus\cdots\oplus P_\nu\oplus W$ と直交和に分解し各 P_i は双曲型平面，W は 0 以外に等方的な元を含まない．

証明 極大な全等方的部分空間の一つを U とおく．この時 $\nu=\dim U$ でさらに $U=\mathrm{rad}\, U$ が成り立つ．したがって (4.3) により双曲型の部分空間

$$U_0=P_1\oplus\cdots\oplus P_\nu$$

が存在する．よって $n\geqq\dim U_0=2\nu$．また U_0 は非等方的であるから

$$V=U_0\oplus W, \quad W=(U_0)^\perp$$

と直交和に分解する．さて W の元 w が等方的と仮定すれば $\langle U, w\rangle$ は全等方的となる．U が極大全等方的部分空間だから $w\in U$．すなわち w は U と W との共通元で $w=0$ となる．▯

注意 内積空間 (V, f) は非退化と仮定する．部分空間 U と W との間に全射同形写像があれば $U^\perp$ と $W^\perp$ との間にも全射同形写像が存在する．これは Witt の定理と同値な命題である．▯

§5 斜 交 群

この節では形式 f が非退化な交代形式である場合を調べよう．定理 3.2 により V の次元は偶数で V は双曲型である．そこで $\dim V=2m$ とおけば

$$V=P_1\oplus\cdots\oplus P_m, \quad P_i=\langle v_i, v_{m+i}\rangle$$

と直交和に分解する．ここで $\{v_i, v_{m+i}\}$ は双曲型の組である．さて

$$B=\{v_1, \cdots, v_m, v_{m+1}, \cdots, v_{2m}\}$$

は V の基であるがこの基に関して f を表現する行列を A とおけば A は

$$A=\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

ここで I は (m, m) 型の単位行列である．$\mathrm{Aut}(V, f)$ は斜交群で

$$\mathrm{Aut}(V, f)=Sp(2m, F)$$

と書くことにする．I §5 で述べたように $Sp(2m, F)$ は

$$S=\{M\in GL(2m, F)\,|\,{}^tMAM=A\}$$

により定義される行列群と同形になる．そこで M を (m, m) 型の小行列に分けて $M\in S$ の条件を書き上げれば次の結果を得る．

$$M=\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}\in S \Longleftrightarrow {}^tM_1M_4-{}^tM_3M_2=I,\quad {}^tM_1M_3,\ {}^tM_2M_4 \text{ は対称行列.}$$

(5.1) $m=1$ の場合 $Sp(2, F)=SL(2, F)$ である．

証明 上の条件式は M の行列式が 1 という条件を表わしている． □

(5.2) 移換 $\tau(\mu, a)$ が交代形式 f に関する等長写像であるための条件は

$$\mu(x)=\lambda f(x, a)$$

となることである．（この条件をみたす移換を**斜交移換**といい $\tau(\lambda, a)$ と書く．）

証明 移換 $\tau=\tau(\mu, a)$ が斜交移換であるための条件は

$$f(\tau x, \tau y)=f(x, y),$$

すなわち，$\mu(y)f(x, a)+\mu(x)f(a, y)=0$ がすべての x, y について成り立つことである．そこで $f(a, y_0)=-1$ となる元 y_0 を一つ定めた上で

$$\lambda=\mu(y_0)$$

とおけば $\mu(x)=\lambda f(x, a)$ となる．逆にこの式をみたす λ について定義される移換は斜交移換であることが容易に確かめられる． □

斜交群 $Sp(2m, F)$ の任意の元 σ について

$$\sigma\tau(\lambda, a)\sigma^{-1}=\tau(\lambda, \sigma a)$$

が成り立つ．よって τ が斜交移換ならば $\sigma\tau\sigma^{-1}$ も斜交移換である．

定理 2.6 に対応する次の定理が成り立つ．

定理 5.3 $Sp(2m, F)$ は斜交移換全体の集合により生成される．

証明 斜交移換全体が生成する部分群を T とおく．

(a)　T が $V-\{0\}$ 上に可移に作用することを証明しよう．$V-\{0\}$ の元 u, v をとる．まず $f(u, v) \neq 0$ と仮定しよう．$\lambda f(u, v)=1$ をみたす λ をとり $a=u-v$ とおいて斜交移換 $\tau=\tau(\lambda, a)$ を考える．この時

$$\tau(u)=u+\lambda f(u, u-v)a=u-a=v$$

となる．さて u, v を $V-\{0\}$ の任意の 2 元とすれば $\langle u\rangle^{\perp}$ と $\langle v\rangle^{\perp}$ に共通な補部分空間がある (I (2.3))．それを $\langle w\rangle$ とおけば

$$f(u, w) \neq 0, \quad f(v, w) \neq 0$$

が成り立つ．したがって斜交移換 τ_1, τ_2 により $\tau_1(u)=w$, $\tau_2(w)=v$ とうつされるから $\tau_2\tau_1(u)=v$ となり (a) が証明される．

(b)　双曲型の組全体のつくる集合を H とおき T が H 上に可移に作用することを証明しよう．(a) により T は $V-\{0\}$ に可移に作用しているから双曲型の組 $\{x, y\}$ と $\{x, z\}$ がある時 $\sigma(x)=x, \sigma(y)=z$ をみたす T の元 σ が存在することを示せばよい．場合を分けてまず $f(y, z) \neq 0$ と仮定する．いま $a=y-z$ とおけば斜交移換 $\tau=\tau(\lambda, a)$ を適当に選んで $\tau(y)=z$ とすることができる ((a)の証明参照)．ところで

$$f(x, a)=f(x, y)-f(x, z)=1-1=0$$

だから $\tau(x)=x$ となる．すなわち τ は $\{x, y\}$ を $\{x, z\}$ にうつす．

次に $f(y, z)=0$ と仮定する．この時 $w=x+z$ とおけば $\{x, w\}$ も双曲型で $f(y, w)=-1$, $f(w, z)=1$ を満足する．したがって前述の通り

$$\tau_3 : \{x, y\} \longrightarrow \{x, w\}, \quad \tau_4 : \{x, w\} \longrightarrow \{x, z\}$$

をみたす斜交移換 τ_3, τ_4 がある．よって積 $\tau_4\tau_3$ は $\{x, y\}$ を $\{x, z\}$ にうつす T の元である．

(c)　双曲型の組 $\{x, y\}$ を一つ定めておく．任意に $\rho \in Sp(2m, F)$ をとれば $\{\rho(x), \rho(y)\}$ は双曲型の組となる．(b) により $\rho(x)=\sigma(x), \rho(y)=\sigma(y)$ を満足する T の元 σ が存在する．したがって $\sigma^{-1}\rho$ は双曲型平面 $P=\langle x, y\rangle$ の各元を不変にしている．$V=P \oplus P^{\perp}$ と直交和に分解するから $\sigma^{-1}\rho$ は $P^{\perp}$ の斜交群の元と見ることができる．よって次元に関する帰納法により定理 5.3 が証明される．□

定理 5.4　$Sp(2m, F) \subset SL(2m, F)$.

証明　移換の行列式の値は 1 だから定理 5.4 は定理 5.3 の系である．□

定理 5.5 $Sp(2m, F)$ の中心は $\{\pm I_{2m}\}$ である.

証明 対称な (m, m) 型行列を B, 任意の (m, m) 型正則行列を A とすれば

$$\begin{pmatrix} I & B \\ 0 & I \end{pmatrix}, \quad \begin{pmatrix} I & 0 \\ B & I \end{pmatrix}, \quad \begin{pmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{pmatrix}$$

は $Sp(2m, F)$ の元である. $Sp(2m, F)$ の中心の元 M を小行列に分けて

$$\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}\begin{pmatrix} I & I \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & I \\ 0 & I \end{pmatrix}\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}$$

などの等式を計算すれば上式より $M_3=0$, $M_1=M_4$ を得る. 同様にして

$$M_4=0, \quad M_1=\lambda I$$

が得られる. ところで $M_1={}^tM_4^{-1}=M_4$ だから $\lambda^2=1$ すなわち斜交群の中心は $\{\pm I_{2m}\}$ と一致する. □

定理 5.6 係数体 F が q 元体である時 $Sp(2m, F)$ の位数は

$$q^{m^2}\prod_{i=1}^{m}(q^{2i}-1).$$

証明 $|Sp(2m, F)|=s_m$ とおく. (5.1) により $s_1=q(q^2-1)$ となり定理 5.6 が $m=1$ の場合に成り立つ. そこで $m>1$ と仮定し帰納法による. V に含まれる双曲型の組の数を h_m とおく. 定理 5.3 の証明 (b) によれば斜交群は双曲型の組の集合に可移に作用し, 一つの双曲型の組の安定化群は $2(m-1)$ 次元の斜交群と同形である(定理 5.3 の証明(c)). したがって等式

$$s_m=h_m s_{m-1}$$

が成り立つ. すなわち h_m が計算できれば上式により s_m が定まる. さて双曲型の組 $\{x, y\}$ において, 第 1 の元 x は 0 以外の任意の元でよいから可能な選び方が $q^{2m}-1$ だけある. 元 x を定めれば y は $f(x, y)=1$ を満足していればよい. x と直交しない元の数は $V-\langle x\rangle^\perp$ の元数 $q^{2m}-q^{2m-1}$ に等しい. そのうち $f(x, y)=1$ をみたす元 y の数は

$$(q^{2m}-q^{2m-1})/(q-1)=q^{2m-1}$$

である. よって $h_m=q^{2m-1}(q^{2m}-1)$ となり定理が成り立つ. □

後章で $Sp(2m, F)$ の中心による商群が三つの例外の場合を除けば単純群であることを証明する. §2 で述べた $PSL(V)$ の単純性と同様な方法を用いて証明することもできる. これについては永尾 [4] を参照されたい.

§6 ユニタリ群

この節では $\theta^2=1$ をみたす係数体 F の自己同形 θ に関する非退化 H 形式を h とし h を不変にするユニタリ群 $U(h)$ を考察する．θ の不変体を F_0 とおく．F が有限体の場合ユニタリ群は h の取り方に関係しないから

$$U(h)=U(n,q) \qquad (n=\dim V, q=|F_0|, q^2=|F|)$$

と表わす．形式 h に対応する行列が逆対角行列，すなわち右上から左下への対角線上に 1 が並びその他は 0 となるものをとれば，有限体上の非退化H形式の指数は極大，すなわち指数は $n/2$ または $(n-1)/2$ となる．以下この節では一般体 F 上のユニタリ群を考えるが h の指数は正と仮定する．H形式や対称形式では指数 0 の場合例外的な性質をもつことが多い．

(6.1) $SU(h)=U(h)\cap SL(V)$ とおけば次式が成り立つ．

$$U(h)/SU(h)\cong\{\alpha\,|\,\alpha\in F, \alpha\theta(\alpha)=1\}.$$

特に F が有限体の場合 $U(h)/SU(h)$ は位数 $q+1$ の巡回群である．

証明　定理 I 5.4 系 1 により $U(h)$ の任意の元 σ は $(\det\sigma)\theta(\det\sigma)=1$ をみたす．そこで F の元 α が $\alpha\theta(\alpha)=1$ をみたしていれば $\det\sigma=\alpha$ となる $U(h)$ の元 σ があることを証明しよう．定理 3.4 により直交基 $\{u_1, \cdots, u_n\}$ をとることができる．いま $\sigma(u_1)=\alpha u_1, \sigma(u_i)=u_i$ $(i\geqq 2)$ とおいて V の線形写像 σ を定義すれば明らかに $\det\sigma=\alpha$，さらに

$$h(\sigma(u_i), \sigma(u_j))=h(u_i, u_j)$$

がすべての i, j について成り立つ．($i=j=1$ の場合 $\alpha\theta(\alpha)=1$ が必要となる．) したがって σ はユニタリ群 $U(h)$ の元となり，前半が証明される．

係数体 F が有限体ならば F^* は巡回群で $\theta(\alpha)=\alpha^q$ $(q=|F_0|)$ が成り立つから後半が容易に証明される．　□

注意　任意の係数体の場合でも (6.1) の後半に相当する結果が成り立つ．いま体 F の標数が 2 でないと仮定すれば $F=F_0(\zeta), \zeta^2=z\in F_0$ をみたす元 ζ をとることができる．この時 $\theta(\zeta)=-\zeta$ だから

$$\alpha=r+s\zeta \qquad (r, s\in F_0)$$

とおけば $\alpha\theta(\alpha)=1$ は $r^2-s^2z=1$ と同値となる．さて $r^2-s^2z=1$ の解 r, s $(r\neq 1)$ に対して $t=sz/(r-1)$ とおけば

$$r=(t^2+z)/(t^2-z), \quad s=2t/(t^2-z)$$

となる．逆に任意の $t\in F_0$ について (r, s) を上のように定義すれば (r, s) は $r^2-s^2z=1$

の解となる．したがって $\alpha=r+s\zeta$ は $\alpha\theta(\alpha)=1$ をみたす．

係 F の標数が2の場合も同様である．F/F_0 はガロア拡大だから

$$F=F_0(\zeta),\quad \zeta^2+\zeta=z\in F_0,\quad \theta(\zeta)=\zeta+1$$

となる(『代数』I, p. 236 定理 4)．この時 $\alpha=r+s\zeta$ が $\alpha\theta(\alpha)=1$ を満足するための条件は $r^2+rs+s^2z=1$ である．この式をみたす $r,s\neq 0$ をとり $t=(r+1)/s$ とおけば

$$r=(t^2+z)/(t^2+t+z),\quad s=1/(t^2+t+z)$$

となる．多項式 X^2+X+z は F_0 上既約だから $t^2+t+z\neq 0$ である．逆に任意の $t\in F_0$ に対し r,s を上のように定義して $\alpha=r+s\zeta$ とおけば，α は $\alpha\theta(\alpha)=1$ を満足する．以上のように F が無限体ならば $\alpha\theta(\alpha)=1$ の解の数は $|F_0|$ に等しい． □

定理 6.2 空間 V の次元が2の場合，h の指数が正ならば

$$SU(h)\cong SL(2, F_0).$$

証明 形式 h は非退化，さらに指数が正と仮定したから (V, h) は双曲型平面である(3.10)．よって双曲型の組 $\{u, v\}$ がある．さて体 F は $\theta(\gamma)=-\gamma$ をみたす元 γ を含んでいる．そこで $\{u, \gamma v\}$ を V の基にとり，h に対応する行列を A とおけば A は

$$\begin{pmatrix} 0 & \theta(\gamma) \\ \gamma & 0 \end{pmatrix}=\begin{pmatrix} 0 & -\gamma \\ \gamma & 0 \end{pmatrix}$$

となる．同じ基により $SU(h)$ の元を行列表示して，それを M とおけば

$${}^tMA\theta(M)=A$$

が成り立つ．$\det M=1$ だから ${}^tMAM=A$ も成り立ち $\theta(M)=M$ を得る．すなわち M の各成分は F_0 の元で $SU(h)=SL(2, F_0)$ となる． □

(6.3) 移換 $\tau=\tau(\mu, a)$ が $U(h)$ の元であるための条件は

$$\mu(x)=\gamma h(x, a),\quad \theta(\gamma)=-\gamma$$

である．特に a は h に関して等方的元である．

証明 τ が h を不変にするための条件はすべての $x, y\in V$ について

$$\mu(x)h(a, y)+\theta(\mu(y))h(x, a)+\mu(x)\theta(\mu(y))h(a, a)=0$$

が成り立つことである．$\mu(a)=0$ だから上式の y に a を代入すれば

$$\mu(x)h(a, a)=0,\quad \text{すなわち}\quad h(a, a)=0$$

となることがわかる．そこで $h(a, y_0)=-1$ をみたす y_0 を一つ定め

$$\gamma=\theta(\mu(y_0))$$

とおけば上式より $\mu(x)=\gamma h(x, a)$ および $\gamma+\theta(\gamma)=0$ を得る．

逆に $h(a,a)=0$ および $\theta(\gamma)=-\gamma$ をみたす元 a,γ をとり

$$\tau(x)=x+\gamma h(x,a)a$$

とおけば τ は $U(h)$ に含まれる移換となる. ▯

上の形に表わされる移換を**ユニタリ移換**といい $\tau=\tau(\gamma,a)$ と表わす. 形式 h の指数が0ならば $U(h)$ は移換を含まない. 指数が正の場合ユニタリ移換全体が生成する部分群を T とおけば次の定理が成り立つ.

定理 6.4 形式 h の指数が正ならば一つの例外を除いて $T=SU(h)$ となる. 例外は $SU(3,2)$ である.

注意 定理6.4の証明の方針は $SL(V)$ や斜交群の場合と同様である. 非等方的な元 u をとり $V=\langle u\rangle\oplus\langle u\rangle^{\perp}$ と直交和に分解する. $SU(h)$ の元 σ を任意にとった時 $\sigma(u)=\tau(u)$ をみたす $\tau\in T$ が存在することを証明する. そうすれば $\tau^{-1}\sigma$ は u を不変にするから $\langle u\rangle^{\perp}$ 上のユニタリ群の元と見ることができる. そこで次元に関する帰納法により $\tau^{-1}\sigma\in T$, したがって $\sigma\in T$ が証明される. しかしユニタリ群の場合, 証明の細部が複雑で面倒である. 係数体が有限体の場合に限定すれば比較的簡単に証明できる. これに関しては永尾 [4] p. 193 を参照されたい. ▯

証明 (a) まず2次元の場合に定理が成り立つことを示そう. 定理6.2によりユニタリ群は $SL(2,F_0)$ と同形である. 定理2.7により $SL(2,F_0)$ は

$$\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\qquad \begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}$$

により生成される. 定理6.2の証明からわかるように双曲型の組 $\{u,v\}$ および $\theta(\gamma)=-\gamma$ をみたす元 γ があって上にあげた行列で表現される $U(h)$ の元はそれぞれユニタリ移換 $\tau(b\gamma,u),\tau(c\gamma,v)$ である. よって2次元の場合に定理が成り立つ.

(b) 以下 $n=\dim V\geqq 3$ と仮定し n に関する帰納法による. まず適当に非等方的元 u を選べば $W=\langle u\rangle^{\perp}$ と W 上への h の制限 h' に対して帰納法が適用できること, すなわち h' の指数が正となることを証明しよう. 仮定により h の指数は正だから等方的元 $v\neq 0$ がある. いま $H=\langle v\rangle^{\perp}$ とおけば H の次元は $n-1$ である. もし H の各元が等方的ならば (3.3) により H は全等方的となる. したがって定理4.9により $n-1\leqq n/2$, すなわち $n\leqq 2$ という矛盾がおこる. よって H は非等方的な元 u を含んでいる. このように元 u を選べば $W=\langle u\rangle^{\perp}$ 上への制限 h' の指数は正となる.

(c) 証明をはじめる前に，非等方的元 w が与えられた時 w を含む双曲型平面が必ずとれることを示そう．仮定により形式 h の指数は正だから等方的な元 x がある．(4.3)により等方的な元 y があって $\{x, y\}$ は双曲型の組となる．さて(3.10)の証明の中で注意したように $h(w, w)=\lambda+\theta(\lambda)$ をみたす F の元 λ が存在する．そこで $w_0=x+\lambda y$ とおけば

$$h(w_0, w_0)=\lambda+\theta(\lambda)=h(w, w)$$

が成り立つ．したがって $\alpha w_0 \to \alpha w$ $(\alpha\in F)$ は $\langle w_0\rangle$ から V の中への等長写像である．Witt の定理によりそれを V の自己同形 φ に拡張できる．そこで φ による $\langle x, y\rangle$ の像を P とおけば P は双曲型平面で w を含んでいる．

(d) 以下，元 u は (b) の条件を満足するように選ばれていると仮定する．しばらくの間 $|F_0|\geqq 5$ と仮定する．まず $\sigma\in SU(h)$ が u を動かさない場合には σ は T の元であることを証明しよう．前のように $W=\langle u\rangle^{\perp}$，$W$ 上への h の制限を h' とおく．元 u が (b) の条件をみたしているから (W, h') について帰納法の仮定が満足される．仮定により σ は u を動かさないから W も不変にし，W 上にユニタリ群 $SU(h')$ の元 σ' を引きおこしている．$|F_0|\geqq 5$ と仮定したから例外の場合は起らず帰納法の仮定により σ' は W 上のユニタリ移換の積となる．ところで W 上のユニタリ移換は (u を動かさずに) V 上のユニタリ移換に拡張されるから ((4.5)参照) σ がユニタリ移換の積となる．すなわち $\sigma\in T$ が成り立つ．

(e) $SU(h)$ の任意の元 σ をとる．この時 $\sigma(u)=\tau(u)$ をみたす $\tau\in T$ が存在することをいくつかの場合に分けて証明する．前に注意したように，これから $\sigma\in T$ が得られるから定理が成り立つ．まず $\sigma(u)$ と u とを含む双曲型平面 P が存在する場合を考えよう．$\alpha u \to \alpha\sigma(u)$ は $\langle u\rangle$ から P の中への等長写像だから Witt の定理によりそれを P の自己同形 φ に拡張することができる．ここで φ の行列式の値を1にとれることを証明しよう．$\sigma(u)$ は非等方的だから $\sigma(u)$ を一員とする P の直交基 $\{\sigma(u), v\}$ がある(定理 3.4)．いま $\gamma\det\varphi=1$ をみたす元 $\lambda\in F$ をとれば $\sigma(u)\to\sigma(u), v\to\lambda v$ により定義される線形写像 ψ はユニタリ群の元で $\det\psi=\lambda$ となる(6.1)．よって φ の代りに $\psi\varphi$ をとれば $\psi\varphi$ も u を $\sigma(u)$ にうつし，行列式の値が1となる．(a) により $\psi\varphi$ は P のユニタリ移換の積となる．(d) と同様に P のユニタリ移換は ($P^{\perp}$ の元を動か

さずに) V のユニタリ移換に拡張されるから $\psi\varphi$ は T の元 τ に拡張される．よって $\sigma(u)=\tau(u),\ \tau\in T$ となる．

(f) $w=\sigma(u)-u$ とおき w が非等方的と仮定する．w を含む双曲型平面を一つ定めそれを P とおく．元 u の P への射影を x とし

$$u=x+y \qquad (x\in P, y\in P^{\perp})$$

とおく．ここで x が非等方的ならば $\sigma(u)=\tau(u), \tau\in T$ をみたす τ が存在することを証明しよう．定義から $\sigma(u)=w+x+y$ となる．よって

$$h(u, u)=h(\sigma(u), \sigma(u)) \Longrightarrow h(x, x)=h(w+x, w+x)$$

を得る．仮定により $w\in P$ で P は双曲型だから $\rho(x)=w+x$ をみたす $SU(P)$ の元 ρ が存在する．((e) の証明参照．元 x が非等方的だから ρ の行列式の値を1にできる.) 前と同様 $P^{\perp}$ の元は動かさずに ρ を $SU(h)$ の元 τ に拡張できる．そうすれば $\tau\in T$．さらに $\tau(y)=y$ より

$$\tau(u)=\tau(x+y)=w+x+y=\sigma(u)$$

となり τ は求めていた元である．よってこの場合 $\sigma\in T$ が成り立つ．

(g) この項では引き続いて $w=\sigma(u)-u$ が非等方的と仮定する．前項 (f) において $u=x+y$ と分解した時 x が等方的ならば，w を含む双曲型平面をとりかえて (f) の条件が満足されるようにできることを示そう．元 w は非等方的と仮定したから $h(w, w)\neq 0$，すなわち

$$h(w, \sigma(u))\neq h(w, u)$$

を得る．さて $h(w, u)=0$ ならば $h(\sigma(u), u)=h(u, u)=h(\sigma(u), \sigma(u))$．よって $h(\sigma(u), w)=0$ となる．しかしこれは上の不等式に矛盾するから

$$h(w, u)\neq 0$$

が成り立つ．そこで

$$u=a+b \qquad (a\in\langle w\rangle, b\in\langle w\rangle^{\perp})$$

と分解すれば $a\neq 0$ である．さらに $h(a, a)\neq 0$ が成り立つ (w が非等方的と仮定している)．いま

$$\alpha=h(a, a), \quad \beta=h(b, b), \quad x=a+c$$

とおけば $\alpha\neq 0$．また $c=b-y$ より $c\in\langle w\rangle^{\perp}$ を得る．特に

$$h(a, b)=h(a, c)=0$$

が成り立つ．元 x は等方的だから $h(c, c)=-h(a, a)=-\alpha$．ここで

$$d=\lambda b+\mu c$$

を適当に選べば $P'=\langle a, d\rangle$ は w を含む双曲型平面で，この P' により

$$u=x'+y' \qquad (x'\in P', y'\in(P')^{\perp})$$

と分解すれば x' が非等方的になることを証明しよう．そのために

$$e=a+d$$

とおけば $h(a, d)=0$ より $h(e, a)=h(a, a)=\alpha\neq 0$ を得る．そこで e が等方的ならば P' は双曲型となる(3.10)．元 e が等方的であるための条件は $(d, d)=-\alpha$ である．$c=x-a\in P$ より $h(c, y)=0$，よって

$$h(b, c)=h(c, b)=h(c, c)=-\alpha$$

を得る．したがって e が等方的となるための条件は

$$(*) \qquad \beta\lambda\theta(\lambda)-\alpha(\lambda\theta(\mu)+\theta(\lambda)\mu+\mu\theta(\mu))=-\alpha$$

が成り立つことである．ここで $\gamma=(\alpha+\beta)/\alpha$ とおけば上式（$*$）は

$$(*)' \qquad \gamma\lambda\theta(\lambda)+1-(\lambda+\mu)\theta(\lambda+\mu)=0$$

と書き直すことができる．この条件をみたす元 d を選べば $P'=\langle a, d\rangle$ は双曲型平面で，さらに $\lambda\neq 0$ ならば $P'\neq P$ となる．さて $u=x'+y'$ と分解した時 x' が等方的と仮定すれば

$$x'=\xi(a+\rho d), \quad \rho\theta(\rho)=1 \qquad (\xi\in F)$$

と書ける．さらに $h(x', u)=h(x', x')=0$ が成り立つ．いま $\rho\theta(\rho)=1$ をみたす元 ρ をどのようにとっても $h(a+\rho d, u)\neq 0$ となるように d を選ぶことができれば，この元 d により定められる双曲型平面 P' への u の射影は非等方的となり前項 (f) の仮定が満足される．さて

$$h(a+\rho d, u)=\alpha+\rho(\lambda\beta-\mu\alpha)$$

となるから $\delta=\mu-\lambda(\beta/\alpha)$ とおいた時 $\delta\theta(\delta)\neq 1$ をみたすように μ, λ を選べば必ず $h(a+\rho d, u)\neq 0$ となる．そこで $\alpha^2\delta\theta(\delta)$ を展開して条件($*$)を用いれば $\delta\theta(\delta)\neq 1$ は $\alpha(\alpha+\beta)(\mu\theta(\mu)-1)\neq 0$ と同値になる．ところで $\alpha\neq 0$, $\alpha+\beta=h(u, u)\neq 0$ だから $\delta\theta(\delta)\neq 1$ は

$$\mu\theta(\mu)\neq 1$$

と同値になる．この条件と($*$)とを同時に満足する λ, μ があることを示そう．

まず体 F の標数が2でない場合を考えよう．この時

$$F=F_0(\zeta), \quad \zeta^2=z\in F_0, \quad \theta(\zeta)=-\zeta$$

となる．そこで $\lambda=q+r\zeta, \lambda+\mu=s+t\zeta$ $(q, r, s, t\in F_0)$ とおけば条件 $(*)'$ は $\gamma(q^2-r^2z)+1-s^2+t^2z=0$ となる．$s=1, q=r=t=0$ 以外の解を求めるため $q=\xi(s-1), r=0, t=\eta(s-1)$ とおけば

$$(\gamma\xi^2+\eta^2z)(s-1)=s+1$$

を得る．そこで $\xi\neq 0, \gamma\xi^2+\eta^2z\neq 1$ をみたす F_0 の元 ξ, η をとれば上式をみたす $s\in F_0$ が定まる．体 F の標数は 2 でないと仮定したから $s\neq 1$．よって $\lambda=\xi(s-1)\neq 0$ となる．また $\mu=s-q+t\zeta$ だから

$$\mu\theta(\mu)=[s-\xi(s-1)]^2-\eta^2(s-1)^2z\neq 1$$

を得る．ここで $s-1$ で割り，上に求めた s の値を代入して式を簡約すれば

$$(\xi-1)(1-\gamma\xi)\neq\eta^2z$$

と同値になる．そこで $\xi\neq 0$ を一つ定めれば η は二つの 2 次不等式を満足するようにとればよい．$|F_0|\geqq 5$ と仮定してあるからこれらの制限をみたす ξ, η は存在し，したがって条件（$*$）および $\mu\theta(\mu)\neq 1$ をみたす λ, μ がある．

体 F の標数が 2 の場合も同様である．この時は

$$F=F_0(\zeta),\quad \zeta^2+\zeta=z\in F_0,\quad \theta(\zeta)=\zeta+1$$

となる(『代数』 I, p. 236)．前のように q, r, s, t を定めれば条件 $(*)'$ は

$$\gamma(q^2+qr+r^2z)+1-(s^2+st+t^2z)=0$$

と表わせる．そこで $q=\xi(s-1), r=0, t=\eta(s-1)$ とおけば

$$(\gamma\xi^2+1+\eta^2z)(s-1)+s\eta=0$$

となる．前のように $\xi\neq 0, \gamma\xi^2+1+\eta^2z+\eta\neq 0$ としさらに $\eta\neq 0$ とすれば上式より $s\neq 1$ を得るから $\lambda=\xi(s-1)\neq 0$ が成り立つ．さて

$$\mu\theta(\mu)=(q+s)^2+(q+s)t+t^2z\neq 1$$

となるための条件は ($s-1$ で割ったあと s の値を代入して整理すれば)

$$\xi\eta(\gamma\xi+\xi+\eta)\neq 0$$

となる．ところで $\xi\eta\neq 0$ だから $\gamma\xi+\xi+\eta\neq 0$ を得る．よって ξ の値を一つ定めれば上の三つの不等式をみたす η が存在し($|F_0|\geqq 5$)，したがって条件（$*$）および $\mu\theta(\mu)\neq 1$ をみたす λ, μ が存在する．

(h) 前項 (g) および (f) において $w=\sigma(u)-u$ が非等方的な場合の証明が終了したから今度は w が等方的と仮定する．

さて $h(u, \sigma(u))=0$ ならば u と $\sigma(u)$ とが生成する平面は非退化で等方的な

元を含んでいる．よってそれは双曲型となり (e) により定理が成り立つ．

そこで $h(u,\sigma(u))=\gamma$ とおき $\gamma\neq 0$ と仮定する．この時 $\lambda\theta(\lambda)=1$ をみたす元 λ を適当に選べば $\sigma(u)-\lambda u$ が非等方的になることを証明しよう．仮定により w は等方的だから $h(w,w)=0$ を展開して

$$2h(u,u)=\gamma+\theta(\gamma)$$

を得る．いま $\lambda\theta(\lambda)=1$ をみたす元 λ について $\sigma(u)-\lambda u$ が等方的なら

$$\lambda\gamma+\theta(\lambda\gamma)=h(\sigma(u),\sigma(u))+h(\lambda u,\lambda u)=\gamma+\theta(\gamma)$$

となる．すなわち λ は2次式 $\lambda^2\gamma-\lambda(\gamma+\theta(\gamma))+\theta(\gamma)=0$ をみたす．ところで $\gamma\neq 0$ だからこのような λ は高々二つしかない．一方，前に注意したように ((6.1)のあと) $\lambda\theta(\lambda)=1$ をみたす元は少なくとも三つある．よって適当に λ を選んで $\lambda\theta(\lambda)=1$，さらに $w'=\sigma(u)-\lambda u$ が非等方的となるようにできる．

元 u は非等方的だから，u を含む双曲型平面 P がある ((c) 参照)．よって，$\lambda u\to u$ を $SU(P)$ の元に拡張できる ((e) 参照)．すなわち $\tau\in T$ があって $\tau(\lambda u)=u$ となる．さて σ の代りに $\tau\sigma$ を考えれば

$$\tau\sigma(u)-u=\tau(\sigma(u)-\lambda u)=\tau(w')$$

となり $\tau(w')$ は非等方的である．(f) および (g) により $\tau\sigma$ について定理が成り立つ．したがって $\sigma\in T$ となり定理が証明される．

(i)　以下 $|F_0|=q\leqq 4$ と仮定する．この時も $n=4, q=2$ の場合を除けば帰納法が適用され (d) で証明した命題が成り立つ．非等方的な元 u を前のように定める．任意の $\sigma\in SU(h)$ について，$n=3, q=2$ の場合を除けば

$$\sigma(u)=\tau(u),\quad \tau\in T$$

をみたす元 τ が存在することを証明しよう．この場合も (e) で扱った場合はそのまま成立する．よって u と $\sigma(u)$ とが双曲型でない平面 P を生成する場合だけ考えればよい．ところで有限体上では非退化な平面はすべて双曲型だから P は退化している．そこで

$$\sigma(u)=\lambda u+v$$

とおいて v が $\mathrm{rad}\,P$ を生成するようにできる．(4.3) により

$$V=\langle u\rangle\oplus\langle v,v'\rangle\oplus V'$$

と直交和に分解し $\{v,v'\}$ は双曲型の組となる．ここで $n\geqq 4$ ならば V' は $\{0\}$ でない非退化部分空間である．したがって V' は $h(w,w)=h(u,u)$ をみ

たす元 w を含んでいる．この時 $\langle u, w\rangle$, $\langle w, \sigma(u)\rangle$ は共に双曲型平面だから (e) により

$$\tau_1(u)=w, \quad \tau_2(w)=\sigma(u)$$

をみたす元 $\tau_1\in T$, $\tau_2\in T$ がある．よって $\tau_2\tau_1(u)=\sigma(u)$ となり $\tau_2\tau_1$ は T の元である．次に $n=3, q>2$ と仮定すれば $\beta\theta(\beta)\neq h(u,u)^2$ をみたす元 $\beta\neq 0$ がある(3.6)．この β に対し $\alpha\theta(\beta)+\theta(\alpha)\beta=h(u,u)$ をみたす α が存在する．そこで $w=\alpha v+\beta v'$ とおけば

$$h(w,w)=\alpha\theta(\beta)+\theta(\alpha)\beta=h(u,u), \quad h(w,u)=0$$

となる．また $\sigma(u)=\lambda u+v$ だから $h(w,\sigma(u))=\beta$ を得る．よって β の定義から $\langle w, \sigma(u)\rangle$ は非退化な平面となる．よって $\langle u, w\rangle, \langle w, \sigma(u)\rangle$ は共に双曲型平面だから前と同様に $\sigma(u)=\tau(u)$ をみたす $\tau\in T$ がある．

(j) 残っているのは $n=4$, $q=2$ の場合 $\sigma(u)=u$ をみたす $SU(h)$ の元 σ が T の元となることの証明である．ここで一般性を失わずに u は V の正規直交基 $\{u, u_1, u_2, u_3\}$ の1元と仮定できる．σ は $W=\langle u\rangle^\perp$ を不変にするから

$$\sigma(u_1)=a_1u_1+a_2u_2+a_3u_3$$

となる．以下 $\tau\in T$ があって $\tau(u)\in\langle u\rangle, \tau\sigma(u_1)\in\langle u_1\rangle$ となることを証明する．これが成り立てば $\rho=\tau\sigma$ は $\langle u, u_1\rangle$ を不変にするから $\langle u, u_1\rangle^\perp=\langle u_2, u_3\rangle$ も不変にする．よって (a) により $\rho\in T$ となり σ が T の元となる．

まず $a_1=0$ と仮定すれば $h(u_1, \sigma(u_1))=0$ だから $\langle u_1, \sigma(u_1)\rangle$ は双曲型平面である．よって W 上のユニタリ移換の積となる元 τ があって

$$\tau\sigma(u_1)=u_1$$

となる．この時 τ は u を動かさずに V 上のユニタリ移換の積に拡張できるから上の命題が成り立つ．

次に $a_2=0$ とすれば $\langle u_1, u_2\rangle, \langle u_2, \sigma(u_1)\rangle$ は共に双曲型平面だから上と同様に命題が証明される．$a_3=0$ の場合も同様である．

最後に $a_i\neq 0$ $(i=1,2,3)$ と仮定する．u_2, u_3 の代りに a_2u_2, a_3u_3 を基の元にとれるから $a_2=a_3=1$ と仮定してもよい．そこで

$$\sigma(u_1)=\alpha u_1+u_2+u_3 \qquad (\alpha\neq 0)$$

とおく．いま $v_1=u+u_1+u_2+u_3, v_2=\beta u+\beta_1u_1+\beta_2u_2+\beta_3u_3$ とおき $\beta, \beta_1, \beta_2, \beta_3$ は0でないとすれば v_1, v_2 は等方的元で

$$\tau_i(x)=x+h(x,v_i)v_i \qquad (i=1,2)$$

はユニタリ移換である(6.3)．$\tau_2\tau_1(u_1)$ を計算すれば

$$\tau_2\tau_1(u_1)\in W \Longleftrightarrow \beta_2=\beta_3$$

を得る．この時

$$\tau_2\tau_1(u)=\beta\theta(\beta_1)u+(1+\theta(\beta_1)\beta_2)(u_2+u_3)$$

$$\tau_2\tau_1(u_1)=\theta(\beta)\beta_1u_1+(1+\theta(\beta)\beta_2)(u_2+u_3)$$

となる．そこで F の生成元を γ として $\beta=\gamma, \beta_1=\beta_2=\beta_3=1$ とおけば

$$\tau_2\tau_1(u)=\gamma u, \quad \tau_2\tau_1(u_1)=\gamma(\gamma u_1+u_2+u_3)$$

を得る．上の $\sigma(u_1)$ と較べてみれば，$\alpha\neq 1$ の場合には $\alpha=\gamma$ ととれるから $\tau=(\tau_2\tau_1)^{-1}$ が条件をみたしている．一方，$\alpha=1$ の場合には

$$\tau_3: u \longrightarrow \gamma u, \quad u_1 \longrightarrow \gamma^{-1}u_1, \quad u_2 \longrightarrow u_2, \quad u_3 \longrightarrow u_3$$

により τ_3 を定義する．(a) により τ_3 もユニタリ移換の積となり

$$\rho=\tau_3\tau_2\tau_1: u \longrightarrow \gamma^2 u, \quad u_1 \longrightarrow \gamma(u_1+u_2+u_3)$$

が成り立つ．よって $\tau=\rho^{-1}$ が求める元となる．

以上で定理 6.4 が証明された． □

最後に有限体上のユニタリ群の位数を求めよう．定理 5.6 の証明と同様の方法を用いる．

(6.5) 有限体 $GF(q^2)$ 上の n 次元線形空間 V で定義された非退化 H 形式を h とする．V に含まれている等方的元の数を s_n とおけば

$$s_n-1=(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)$$

が成り立つ．

証明 定理 3.7 により V は正規直交基 $\{v_1, \cdots, v_n\}$ をもっている．そこで $x=\lambda v_1+v$ $(v\in\langle v_1\rangle^\perp)$ とおけば

$$h(x,x)=\lambda\theta(\lambda)+h(v,v)$$

が成り立つ．いま $\lambda=0$ の場合と $\lambda\neq 0$ の場合にわけて等方的元の数を数えれば $s_n=s_{n-1}+(q^2-1)(q^{2(n-1)}-s_{n-1})/(q-1)$ を得る．明らかに $s_1=1$ だから $n=1$ の時 (6.5) が成り立つ．帰納法により (6.5) が証明される． □

(6.6) 前命題と同じ記号を用いる．V に含まれる双曲型の組の数を h_n とおけば次式が成り立つ．

$$h_n=(s_n-1)q^{2n-3}$$

証明 まず $n=2$ の場合を考えよう．双曲型の組 $\{x, y\}$ において最初の元には 0 以外の等方的元を任意に選ぶことができる．さて x を一つ定めれば

$$z=\alpha x+\beta y$$

とおいた時 $\{x, z\}$ が双曲型の組となるための条件は

$$h(x, z)=1, \quad h(z, z)=0$$

であるから $\beta=1$ および $\alpha+\theta(\alpha)=0$ を得る．したがって V には双曲型の組が丁度 $(s_2-1)q$ 組存在する．

以下 $n\geqq 3$ と仮定する．等方的元 $x\neq 0$ を定め，x を始めの元とする双曲型の組の数を計算しよう．いま $h(x, z)\neq 0$ をみたす元 z を任意にとれば x と z から生成される平面は非退化となるからそれは双曲型である．したがって x を含む双曲型平面の数は

$$(q^{2n}-q^{2(n-1)})/(q^4-q^2)=q^{2n-4}$$

である．各双曲型平面の中に $\{x, y\}$ が双曲型の組となる元 y が丁度 q 個ずつ含まれているから (6.6) が成り立つ． □

定理 6.7 有限体 $GF(q^2)$ 上のユニタリ群の位数は次式で与えられる．

$$|U(n, q)|=q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-(-1)^i).$$

証明 $\{x, y\}$ を双曲型の組とする．任意に双曲型の組 $\{x', y'\}$ をとれば対応 $x\to x', y\to y'$ は $\langle x, y\rangle$ から V の中への等長写像を与えるから，Witt の定理によりそれをユニタリ群の元に拡張することができる．すなわちユニタリ群 $U(n, q)$ は双曲型の組全体のつくる集合に可移に作用している．

組 $\{x, y\}$ の安定化群は $V'=\langle x, y\rangle^{\perp}$ 上のユニタリ群で $U(n-2, q)$ と同形になる．したがって

$$|U(n, q)|=h_n|U(n-2, q)|$$

を得る．$n=1, 2$ の場合に定理 6.7 が成り立つから帰納法および (6.6) により一般に定理が成り立つ． □

§7 直 交 群

1. 2次形式による内積空間 これまで直交群を考える場合，係数体 F の標数は 2 でないと仮定し非退化対称形式 f をもとにして直交群を定義した．しかし直交群は 2 次形式を不変にする群としても定義される．この方法によれば

係数体の標数に関係なく理論が構成されるので，この節では2次形式から出発して直交群を定義しよう．

定義 7.1 線形空間 V の上で定義された**2次形式**とは，V 上で定義され係数体 F の中に値をとる関数 Q で次の性質をもつものと定義する．

(1) 任意の $u\in V$ と $\lambda\in F$ に対して $Q(\lambda u)=\lambda^2 Q(u)$ が成り立つ．

(2) 任意の $u\in V$ と $v\in V$ に対して

$$f(u, v)=Q(u+v)-Q(u)-Q(v)$$

とおけば f は $V\times V$ で定義された双線形形式である．

この時 f を Q に**同伴する双線形形式**という． □

条件(2)により Q の同伴双線形形式 f は

$$f(u, v)=f(v, u)$$

をみたす．すなわち，同伴形式は対称である．また(1), (2)から

$$f(u, u)=2Q(u) \tag{7.2}$$

が成り立つ．したがって係数体 F の標数が2の場合 f は交代形式となる．係数体の標数が2でなければ2次形式 Q は同伴形式 f により一意的に定まる．空間 V に基 $\{u_1, u_2, \cdots, u_n\}$ をとれば F の任意の元 $a_1, a_2, \cdots, a_n$ に対して

$$Q(\sum_i a_i u_i)=\sum_i a_i{}^2 Q(u_i)+\sum_{i<j} a_i a_j f(u_i, u_j) \tag{7.3}$$

が成り立つ．したがって標数2の場合も f および $Q(u_1), \cdots, Q(u_n)$ を与えれば2次形式 Q は一意的に定まる．また $\{Q(u_i)\}$ を任意に与えた時 (7.3) の右辺で定義される関数 Q が同伴形式 f の V 上の2次形式であるための条件は (7.2) が成り立つこと，すなわち $2Q(u_i)=f(u_i, u_i)$ $(i=1, \cdots, n)$ である．

定義 7.4 2次形式 Q の定義されている空間 V も**内積空間**といい前のように (V, Q) と表わす．2次形式 Q が**非退化**であるというのは同伴形式 f が非退化であることと定義する．Q が非退化ならば内積空間 (V, Q) が非退化であるという．$GL(V)$ の元 σ が $Q(\sigma u)=Q(u)$ をみたす時 σ を**等長写像**といい，

$$\mathrm{Aut}(V, Q)=\{\sigma\in GL(V) \mid Q(\sigma u)=Q(u),\ \forall u\in V\}$$

とおく．$\mathrm{Aut}(V, Q)$ を (Q に関する) **直交群**といい $O(Q)$ とも表わす． □

注意 もし $\sigma\in \mathrm{Aut}(V, Q)$ ならば任意の $u, v\in V$ に対して

$$f(\sigma u, \sigma v)=f(u, v)$$

が成り立つ．したがって $\mathrm{Aut}(V, Q)\subset \mathrm{Aut}(V, f)$．係数体の標数が2でなければ Q は f

により定まるから $\mathrm{Aut}(V, Q)=\mathrm{Aut}(V, f)$. 係数体の標数が 2 で Q が非退化であれば同伴形式 f は非退化交代形式で V の次元 n は偶数となる(3.2). この場合, 直交群 $O(Q)$ は斜交群の部分群である. ▯

以下この節では 2 次形式 Q による内積空間だけ考える. この場合, 内積は Q に同伴する双線形形式 f によって与えられていることをあらためて注意しておく. 係数体の標数が 2 の場合 f は交代形式で $f(x, x)=0$ が V のすべての元について成り立つが 2 次形式 Q により元 x の“長さ”$Q(x)$ が別に定められているのである. そこで 2 次形式による内積空間では §3, §4 で定義した概念を多少変更する必要がある.

定義 7.5 2 次形式 Q による内積空間を (V, Q), Q の同伴形式を f とする. V の元 x が $Q(x)=0$ をみたしている時 x を**特異元**という. 部分空間 W の各元が特異である時 W を**全特異**な部分空間という. V の 2 元 x, y が

$$Q(x)=Q(y)=0, \quad f(x, y)=1$$

をみたしている時 $\{x, y\}$ を**強双曲型**の組といい, 強双曲型の組 $\{x, y\}$ が生成する平面を**強双曲型平面**という. 強双曲型平面の直交和となる空間を**強双曲型**という.

(7.6) 2 次形式 Q による内積空間 (V, Q) の部分空間 W が全特異ならば W は (Q の同伴形式 f に関して) 全等方的である.

証明 任意の 2 元 $u, v \in W$ に対して $u+v \in W$ であるから定義式(2)を用いて $f(u, v)=0$ を得る. すなわち W は全等方的である. ▯

注意 係数体の標数が 2 でなければ (7.6) の逆が成り立つ. すなわち全等方的な部分空間は全特異である. 標数 2 の場合, 逆が成り立つとは限らない. 標数が 2 でなければ双曲型の組は強双曲型である(7.2). ▯

まず有限体上で非退化な 2 次形式を分類しよう. 係数体の標数が 2 でない場合は §3 で述べたからここでは係数体は標数 2 の有限体と仮定する.

(7.7) 非退化 2 次形式 Q による内積空間を (V, Q) とし $\dim V>2$ と仮定する. この時, 強双曲型の組がある.

証明 Q の同伴形式を f とすれば f は非退化交代形式である. よって双曲型平面 P があって $V=P\oplus P^{\perp}$ と直交和に分解する. 仮定により $\dim V$ は 2 より大きいから $P^{\perp} \neq \{0\}$ となる. $P^{\perp}$ は非等方的だから $P^{\perp}$ は全特異ではない(7.6). そこで $Q(z) \neq 0$ をみたす $P^{\perp}$ の元 z をとる. P の中に等方的元 $x \neq 0$

をとれば

$$Q(x+\lambda z)=Q(x)+Q(\lambda z)+f(x,\lambda z)=Q(x)+\lambda^2 Q(z)$$

となる．係数体Fは標数2の有限体だから $a=x+\lambda z$ が $Q(a)=0$ をみたすようにλを選ぶことができる．$a\neq 0$ だからaを双曲型の組 $\{a,b\}$ に拡張できる．ここで $\langle a,b\rangle$ が強双曲型であることを証明しよう．いま

$$c=\mu a+b$$

とおけば $f(a,c)=1$ および $Q(c)=Q(b)+\mu$ が成り立つ．よってμを適当に選べば $\{a,c\}$ は強双曲型の組となり，$\langle a,c\rangle=\langle a,b\rangle$． □

(7.8) 2次元の非退化内積空間 (V,Q) において

$$x\neq 0 \Longrightarrow Q(x)\neq 0$$

が成り立つと仮定する．この時 (V,Q) の構造は一意的に定まる．すなわち多項式 $X^2+X+\xi_0$ が $F[X]$ で既約となるξ_0を一つ定めておけばVは次の条件をみたす基 $\{x,y\}$ をもっている．

$$f(x,y)=1,\quad Q(x)=1,\quad Q(y)=\xi_0.$$

証明 任意に $z\neq 0$ をとれば $Q(z)\neq 0$ となる．そこで

$$Q(\lambda z)=\lambda^2 Q(z)=1$$

をみたす $\lambda\in F$ をとり $x=\lambda z$ とおく．Vは非退化だから $f(x,y)=1$ をみたす元yがある．そこで $Q(y)=\xi$ とおいて $Q(tx+y)$ を計算すれば

$$Q(tx+y)=t^2+t+\xi$$

となる．仮定により任意の $t\in F$ について $Q(tx+y)\neq 0$ が成り立つ．よって多項式 $X^2+X+\xi$ は $F[X]$ で既約である．

さて任意の $\alpha\in F$ に対して写像 $\alpha\longmapsto\alpha^2+\alpha$ はFの加法群の自己準同形でその核は $\{0,1\}$ の2元から成る(標数2)．そこでその像をF_1とおけばF_1は加法群Fの指数2の部分群をつくる．多項式 $X^2+X+\xi$ がFで既約であるための条件は $\xi\notin F_1$ である．ところでF_1の指数が2だからこれは

$$\xi\in F_1+\xi_0$$

と同値である．すなわち $\xi=\alpha^2+\alpha+\xi_0$ をみたす $\alpha\in F$ がある．そこでyの代りに $y'=\alpha x+y$ をとれば $Q(y')=Q(\alpha x+y)=\xi_0$ となる．前に述べたようにQはfと $Q(x), Q(y')$ により決定されるから((7.3)参照) 内積空間 (V,Q) は一意的に定まる． □

定理 7.9 標数2の有限体F上の内積空間(V,Q)においてQは非退化2次形式とする．この時 $\dim V=n$ は偶数で $n=2m$ とおけば

$$V=P_1\oplus\cdots\oplus P_{m-1}\oplus P_m$$

と直交和に分解される．ここで $P_1,\cdots,P_{m-1}$ は強双曲型平面，最後のP_mは強双曲型平面であるかまたは (7.8) で定義された平面と同形になる．

証明 次元が偶数であることは前に述べた．もし $n>2$ ならば (7.7) により強双曲型平面P_1があり $V=P_1\oplus(P_1)^\perp$ と直交和に分解する．次元に関する帰納法により $V=P_1\oplus\cdots\oplus P_{m-1}\oplus P_m$ と直交和に分解し $P_1,\cdots,P_{m-1}$ は強双曲型平面となる．最後のP_mは非退化平面である．もしP_mが0以外の特異元を含んでいれば (7.7) の証明を繰り返すことによりP_mが強双曲型となる．一方，P_mの中の特異元は0だけと仮定すればP_mは(7.8)で定義された平面と同形となる．よって定理7.9が成り立つ． ▯

注意 定理3.9および7.9の証明からわかるように係数体が代数的閉体ならば非退化2次形式をもつ偶数次元の空間は強双曲型平面の直交和である． ▯

2. Witt の定理 2次形式による内積空間でも Witt の定理が成り立つ．まず (4.3) が次の形で成立する．

(7.10) 非退化2次形式Qをもつ内積空間を(V,Q)とする．部分空間Uに対し rad U の基 $\{u_1,\cdots,u_r\}$ および rad U の補部分空間 Wが与えられていると仮定し，さらにすべてのiについて $Q(u_i)=0$ と仮定する．この時 (4.3) の結論が成り立ち，すべての i について $\{u_i,v_i\}$ は強双曲型の組となる．

証明 (4.3)の証明と同様で，ただ $\{u_i,v_i\}$ が強双曲型の組となることを証明すればよい．さて $P=\langle u_i,v_i\rangle$ は非退化平面で $Q(u_i)=0$ だからPは強双曲型となる((7.7)の証明参照)．したがって $\{u_i,v_i\}$ が強双曲型となるように元v_iをとることができる． ▯

補題4.5も2次形式の場合に拡張できる．実際

$$Q(\sigma u+\tau w)=Q(\sigma u)+Q(\tau w)+f(\sigma u,\tau w)$$

が成り立つからρが等長写像になる．(4.6) は rad Uが全特異であるという仮定を加えれば2次形式の場合にも成立する．証明には (7.10) を用い，双曲型というところを強双曲型に変更すればよい．

定理4.7の証明では第2の場合，すなわち $x\in D^\perp$ の場合Dが全特異であ

ることを示せば (4.6) の修正が適用されて証明が成り立つ．さて

$$Q(\sigma x-x)=Q(\sigma x)+Q(x)-f(\sigma x, x)=2Q(x)-f(\sigma x, x)$$
$$=f(x, x)-f(\sigma x, x)=f(x-\sigma x, x)$$

だから $x\in D^{\perp}$ から $Q(\sigma x-x)=0$ を得る．D は $\sigma x-x$ で生成されているから D は全特異となる．

定理 4.7 の系および定理 4.9 では等方的を特異と変えればよい．

定義 7.11 非退化な 2 次形式 Q をもつ内積空間 (V, Q) において極大全特異部分空間の次元を Q の**指数**という． ▯

前と同様 $\dim V=n$ の時 Q の指数 ν は不等式 $2\nu\leqq n$ を満足する．係数体 F が有限である時，次元が奇数 $2m+1$ の場合 Q の指数は m，次元が $2m$ であれば Q の指数は m または $m-1$ である(定理 3.11, 3.7, 7.9 参照)．

3. 有限直交群の位数 非退化 2 次形式をもつ内積空間 (V, Q) の次元を n とおく．以下 n が奇数の場合，V が強双曲型の場合，および強双曲型でない場合に分けて考察する．いずれの場合も $n\geqq 3$ であれば

$$V=P\oplus V_1$$

と直交和に分解し P は強双曲型平面，V_1 は V と同種の $n-2$ 次元の内積空間となる．まず V に含まれている特異元の数を計算しよう．

(7.12) 非退化 2 次形式をもつ内積空間 (V, Q) の次元を n, V に含まれている特異元の数を s_n，さらに $q=|F|$ とおく．n が奇数の場合は

$$s_n=q^{n-1}$$

となる．偶数次元の場合 $n=2m$ とおけば

$$s_{2m}=q^{2m-1}+\varepsilon q^{m-1}(q-1),$$

ここで V が強双曲型の時 $\varepsilon=1$，そうでない時は $\varepsilon=-1$ である．

証明 まず $n\geqq 3$ と仮定し $V=P\oplus V_1$ と強双曲型平面 P と V_1 との直交和に分解する．P は $Q(x)=Q(y)=0, f(x, y)=1$ をみたす 2 元 x, y によって生成されている．ここで f は Q の同伴形式である．さて任意に V の元 v をとれば

$$v=\alpha x+\beta y+u \qquad (\alpha, \beta\in F, u\in V_1)$$

と書ける．したがって $Q(v)=\alpha\beta+Q(u)$ となる．よって

$$s_n=(2q-1)s_{n-2}+(q^{n-2}-s_{n-2})(q-1)$$

となる(第 1 項は $Q(u)=0$，第 2 項は $Q(u)\neq 0$ の場合)．整理すれば

$$s_n = q^{n-2}(q-1) + qs_{n-2}$$

となる．奇数次元の場合 $s_1=1$ だから帰納的に $s_n=q^{n-1}$ を得る．2次元の場合，強双曲型ならば $s_2=2q-1$，そうでない場合は $s_2=1$ である．帰納法により (7.12) にあげた s_{2m} の値が得られる．□

次に強双曲型の組 $\{a, b\}$ の数を求めよう．

(7.13) 空間 (V, Q) に含まれている強双曲型の組の数 h_n は次式で与えられる．すなわち $h_n=(s_n-1)q^{n-2}$.

証明 0でない特異元 a を一つ定める．この時 a と直交しない任意の元 x をとれば平面 $\langle a, x\rangle$ は強双曲型である(定理 3.11, 7.9 参照)．その各平面の中に $\{a, b\}$ が強双曲型の組となる元 b が唯一つ存在する．したがって a を定めた上では $\{a, b\}$ が強双曲型となるような b は

$$(q^n - q^{n-1})/(q^2-q) = q^{n-2}$$

個存在する．これから $h_n=(s_n-1)q^{n-2}$ が得られる．□

定理 7.14 非退化2次形式 Q を不変にする有限体 F 上の直交群の位数は次元 n が奇数の場合 ($n=2m+1$ とおき)

$$2q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$$

である．次元が偶数の場合に $n=2m$ とおけば直交群の位数は次の通り．

$$2q^{m(m-1)}\prod_{i=1}^{m-1}(q^{2i}-1)(q^m-\varepsilon).$$

証明 まず $n\geqq 3$ と仮定し $V=P\oplus V_1$ と直交和に分解する．ここで P は強双曲型の組 $\{x, y\}$ を基としている．いま任意に強双曲型の組 $\{a, b\}$ をとれば対応 $x\to a$, $y\to b$ は P から $\langle a, b\rangle$ の上への等長写像に延長される．したがって Witt の定理によりこれを (V, Q) の自己同形に拡張できる．すなわち直交群 $O(Q)$ は強双曲型の組全体のつくる集合に可移に作用している．そこで直交群 $O(Q)$ の中で組 $\{x, y\}$ の安定化群を H とおけば

$$|O(Q):H| = h_n$$

となる(1.10)．この時 H の元は P の各元を不変にするから H は $V_1=P^{\perp}$ を不変にする．いま形式 Q の V_1 上への制限を Q_1 とおけば Q_1 は非退化な2次形式で H は V_1 上の直交群 $O(Q_1)$ の部分群と考えられる．ところで $O(Q_1)$ の任意の元は P の各元を動かさずに $O(Q)$ の元に拡張できるから $H\cong O(Q_1)$ が成

り立つ．したがって $|O(Q)|=h_n|O(Q_1)|$ を用いて帰納法により直交群の位数が計算できる．1次元の場合 $Q(\lambda u)=\lambda^2 Q(u)$ だから直交群の元は

$$u \longmapsto \lambda u \qquad (\lambda=1 \text{ または } \lambda=-1).$$

この場合，係数体の標数は2でないから位数は2である．よって

$$|O(Q)|=2\prod_{i=1}^{m}(q^{2i}-1)q^{2i-1} \qquad (n=2m+1).$$

強双曲型の平面 P には上述のように強双曲型の組が $2(q-1)$ 組ある．したがって P 上の直交群の位数は $2(q-1)$ である．

次に強双曲型でない平面の場合を考える．いま $u\neq 0$ を定めて $Q(u)=\lambda$ とおけば $\lambda\neq 0$ となる．いま $Q(x)=\lambda$ をみたす元 x 全体のつくる集合を L とおく．Witt の定理により直交群 $O(Q)$ が L に可移に作用する．さて平面に基 $\{u, v\}$ を定めれば，元 u の安定化群は v を

$$f(u, v')=f(u, v), \qquad Q(v')=Q(v)$$

をみたす元 v' に動かす．ところで上式をみたす v' は v 以外に唯一つ存在する．($v'=\alpha u+\beta v\neq v$ とおけば上式より $\beta=-1, \alpha\lambda=f(u, v)$ を得る．) したがって元 u の安定化群の位数は2となり直交群の位数は $2|L|$ である．このことから $|L|$ は λ に無関係に定まる．よって直交群の位数は $2(q+1)$ となる．帰納法により

$$|O(Q)|=2(q-\varepsilon)\prod_{i=2}^{m}h_{2i}$$

が成り立つ．ここで $s_{2m}-1=(q^m-\varepsilon)(q^{m-1}+\varepsilon)$ を用いれば定理にあげた公式が証明される．□

系 有限体上で偶数次元の非退化2次形式が同値でない時，それらが定義する直交群は同形ではない．

証明 位数が違っているから同形であり得ない．□

4. 対称変換

定義 7.15 非退化2次形式 Q による内積空間を (V, Q) とする．超平面 H をとり $H^{\perp}$ が非特異な元 z を含んでいると仮定する．この時 H に関する**対称変換**とは

$$s_H : x \longmapsto x-Q(z)^{-1}f(x, z)z$$

と定義する．ここで f は Q の同伴形式である．□

対称変換の定義式において z を λz におきかえても同一の変換が得られる．

したがって対称変換は H だけによって定まり $H^{\perp}$ の元 z の取り方には無関係である．明らかに s_H は線形写像であるが実は次の命題が成り立つ．

(7.16) 対称変換 s_H は直交群 $O(Q)$ の元である．任意の $u \in H$ に対して

$$s_H(u) = u$$

が成り立つ．係数体の標数が 2 でなければ

$$s_H(z) = -z \qquad (z \in H^{\perp})$$

となり特に $\det s_H = -1$ である．標数 2 の場合は $s_H(z) = z$ $(z \in H^{\perp})$ が成り立つ．対称変換 s_H の位数は 2 である．二つの対称変換 s_H と s_K について $H^{\perp} = \langle z \rangle$ および $K^{\perp} = \langle w \rangle$ とおいた時 $f(z, w) = 0$ ならば s_H と s_K とは可換である．すなわち $s_H s_K = s_K s_H$ が成り立つ．

証明 s_H の定義式における z の係数を α とおけば

$$Q(s_H x) = Q(x + \alpha z) = Q(x) + \alpha^2 Q(z) + \alpha f(x, z) = Q(x)$$

が成り立つ．よって s_H は直交群 $O(Q)$ の元である．

さて $u \in H$ ならば $f(u, z) = 0$ だから $s_H(u) = u$ が成り立つ．係数体の標数が 2 でなければ (7.2) より $s_H(z) = z - 2z = -z$ を得る．この元 z に H の基を追加して V の基が得られるから $\det s_H = -1$ となる．標数 2 の場合は $s_H(z) = z$ が成り立つ．したがっていずれの場合でも

$$(s_H)^2(x) = s_H(x + \alpha z) = s_H(x) - \alpha z = x$$

が成り立ち $(s_H)^2 = 1$ を得る．二つの対称変換 s_H と s_K について上の条件が成り立っている時 $s_K(x) = x + \beta w$ とおけば

$$s_H s_K(x) = s_H(x + \beta w) = x + \alpha z + \beta w = s_K s_H(x)$$

となる．よって s_H と s_K は交換可能である． □

任意の $\tau \in O(Q)$ に対し

(7.17) $$\tau s_H \tau^{-1} = s_{\tau H}$$

が成り立つ．これは $Q(z) = Q(\tau z)$ などから明らかであろう．

この節の目標は次の定理の証明である．

定理 7.18 直交群 $O(Q)$ は一つの例外を除いて対称変換全体のつくる集合から生成される．例外は 2 元体上の強双曲型 4 次元空間である．

この定理の証明にあたり対称変換全体が生成する $O(Q)$ の部分群を G_0 とおく．(7.17) により $G_0 \lhd O(Q)$ となる．等式 $G_0 = O(Q)$ が目標である．まず次

の補題を証明しよう．

(7.19) 部分群 G_0 は極大全特異部分空間全体の集合に可移に作用する．

証明 極大全特異部分空間 N と N' を任意にとった時 $N \neq N'$ ならば

$$\dim(N \cap s(N')) > \dim(N \cap N')$$

をみたす対称変換 s があることを示せばよい．仮定により $N+N' \neq N$ となるから $N+N'$ は全特異ではない．したがって $z=x+x'$ $(x \in N, x' \in N)$ をみたす非特異元 z が存在する．この時 $z \notin N$ だから $x' \notin N$ となる．さて

$$H = \langle z \rangle^{\perp}, \quad s = s_H$$

とおけば $s(x') \in N$ が成り立つ．それは $Q(z)=f(x, x')$ より

$$s(x') = x' - Q(z)^{-1} f(x', z) z = x' - z = -x \in N$$

を得るからである．ところで $N \cap N' \subset H$ であるから s は $N \cap N'$ の各元を不変にする(7.16)．したがって $N \cap s(N') \supsetneqq N \cap N'$ が成り立つ． ▯

任意の $\sigma \in O(Q)$ に対し σ による不変元全体のつくる部分空間を $L(\sigma)$，その次元を $d(\sigma)$，さらに $u_\sigma = \sigma - 1$ とおく．ここで $u_\sigma(V)$ が全特異となる元 σ を**特異元**と呼ぶことにする．

(7.20) 部分群 G_0 の各剰余類は特異元を含む．

証明 剰余類の代表 σ を $d(\sigma)$ が最大となるように選ぶ．この時 σ が特異元であることを証明しよう．さて σ が特異元ではないと仮説をたてれば $u_\sigma(V)$ は非特異元 $z=\sigma(y)-y$ を含んでいる．そこで $\langle z \rangle^{\perp}$ に関する対称変換を s とおく．(7.2) を用いて

$$Q(z) = 2Q(y) - f(\sigma(y), y) = -f(z, y)$$

が得られるから $s(y) = y - Q(z)^{-1} f(y, z) z = y + z = \sigma(y)$ となる．一方，

$$f(\sigma(x), \sigma(y)) = f(x, y)$$

が成り立つから $x \in L(\sigma)$ ならば $x \in \langle z \rangle^{\perp}$ を得る．よって

$$\langle L(\sigma), y \rangle \subset L(s^{-1}\sigma)$$

となる．ところで $y \notin L(\sigma)$, $s^{-1}\sigma \in G_0\sigma$ だから，上式は $d(\sigma)$ を最大にとったことに矛盾する．よって σ は特異元である． ▯

極大な全特異部分空間 N を一つ定め $N^{\perp}$ の各元を不変にする $O(Q)$ の元全体のつくる部分群を H とおく．N の基 $\{u_1, u_2, \cdots, u_n\}$ を任意にとれば(7.10)の条件を満足する $\{v_1, v_2, \cdots, v_n\}$ が存在する．そこで

$$P=\langle v_1, v_2, \cdots, v_n\rangle$$

とおけば $P\cap N^{\perp}=\{0\}$ かつ (7.3) により P は全特異である．また

$$V=(N^{\perp})+P$$

と直和に分解する．ここで次の補題が成り立つことを証明しよう．

(7.21) (i) 任意の $s\in H, y\in P, z\in P$ に対して

$$g_s(y, z)=f(y, s(z))$$

とおけば g_s は P 上で定義された交代形式である．

(ii) 写像 $s\longmapsto g_s$ は H から交代形式のつくる加法群の中への単射準同形である．特に H は可換群である．

(iii) g_s と g_t の階数が等しければ，H の元 s と t は $O(Q)$ の中で共役である．(形式 g の**階数**とは $\mathrm{rad}(P, g)$ の余次元である．)

(iv) $O(Q)$ の任意の特異元は G_0 の元により H の元と共役になる．

(v) $O(Q)=HG_0$ が成り立つ．商群 $O(Q)/G_0$ は可換群である．

証明 (i) 任意の $s\in H, x\in N^{\perp}, y\in P$ に対して

$$f(x, y)=f(sx, sy)=f(x, sy)$$

が成り立つ．したがって $y-sy\in(N^{\perp})^{\perp}=N$ を得るから

$$0=Q(y-sy)=Q(y)+Q(sy)-f(y, sy)$$

となる．$Q(y)=Q(sy)=0$ だから $f(y, sy)=0$ を得る．すなわち形式 g_s は交代形式である．

(ii) 任意の $s\in H, t\in H, y\in P, z\in P$ に対して $tz-z\in N$ だから

$$s(tz-z)=tz-z$$

を得る．したがって $stz=sz+tz-z$．さて $f(y, z)=0$ だから

$$g_{st}(y, z)=f(y, (st)z)=g_s(y, z)+g_t(y, z),$$

すなわち $g_{st}=g_s+g_t$ が成り立つ．もし $g_s=0$ ならば

$$0=g_s(y, z)=f(y, sz)=f(y, sz-z)$$

が任意の $y\in P, z\in P$ について成り立つ．よって $sz-z\in P^{\perp}$ となる．ところで $sz-z\in N$ も成り立つから $sz-z\in N\cap P^{\perp}=\{0\}$．すなわち s は恒等写像である．よって $s\longmapsto g_s$ は単射準同形である．

(iii) 階数 2ρ の交代形式 g に対して P の基 $\{y_1, \cdots, y_r\}$ を

$$g(y_{2i-1}, y_{2i})=-g(y_{2i}, y_{2i-1})=1 \qquad (i\leqq\rho)$$

その他の i,j について $g(y_i,y_j)=0$ となるように選ぶことができる．形式 f により $N\cong P^*$ となるから N の基 $\{x_1,\cdots,x_r\}$ を

$$f(x_i,y_j)=\delta_{ij} \qquad (\delta_{ii}=1,\delta_{ij}=0\ (i\neq j))$$

をみたすようにとる．さて $g=g_t$ $(t\in H)$ であれば定義から

$$(*)\qquad \begin{aligned} &t(y_{2i-1})=y_{2i-1}-x_{2i}, \quad t(y_{2i})=y_{2i}+x_{2i-1} \qquad (i\leqq\rho) \\ &t(y_j)=y_j \qquad (j>2\rho) \end{aligned}$$

を得る．いま $t'\in H$ に対応する交代形式の階数がやはり 2ρ であるとすれば t' に対応して P の基 $\{y_i'\}$，N の基 $\{x_i'\}$ が上のように定まる．対応

$$x_i\longmapsto x_i',\quad y_i\longmapsto y_i'$$

は $N+P$ の等長写像を与えるから，それを V の等長写像 s に拡張できる．上述のように t,t' はそれぞれの基の上で同一の作用をするから $t'=sts^{-1}$ となる．すなわち t と t' は $O(Q)$ の中で共役となる．

(iv)　任意の特異元を s とする．定義により $u_s(V)$ は全特異であるから極大全特異部分空間 N' があって $u_s(V)\subset N'$ となる．(7.19) により $N=t(N')$ をみたす G_0 の元 t がある．ところで任意の $x\in V,y\in(N')^\perp$ に対し

$$f(sx-x,y)=f(sx,y-sy)=0$$

が成り立つ $(u_s(V)\subset N')$．したがって $y\in L(s)$ を得る．すなわち

$$(N')^\perp\subset L(s)$$

となる．よって $N^\perp=t(N')^\perp\subset tL(s)=L(tst^{-1})$ が成り立つ．これは tst^{-1} が H の元であることを示している．

(v)　任意の剰余類は特異元 σ を含む (7.20)．ところで (iv) により

$$t\sigma t^{-1}\in H \qquad (t\in G_0)$$

となるから $G_0\sigma\subset HG_0$，すなわち $O(Q)=HG_0$ を得る．同形定理と (ii) から商群 $O(Q)/G_0$ が可換群であることが証明される．□

定理 7.18 の証明　任意の元 $s\in H$ をとり対応する交代形式を $g=g_s$ とおく．任意の $\lambda\in F^*$ に対し λg は交代形式でその階数は g の階数と一致する．ここで $\lambda g=g_t$ をみたす H の元 t が存在することを証明しよう．

形式 λg に対し P,N の基を (7.21) (iii) の証明のようにとり，(＊) によって写像 t を P 上で定義する．明らかに $y\in P$ ならば $Q(ty)=Q(y)$ が成り立つ．さらに $ty-y\in N$ だから任意の $x\in N^\perp$ について

$$f(x, ty)=f(x, y)$$

となる．したがって2次形式の場合の (4.5) が適用され，t は V 上の等長変換に拡張できる． この拡張は $N^{\perp}$ の各元を不変にするから H の元である． 定義から明らかに $\lambda g=g_t$ が成り立つ．

まず $|F|\geqq 3$ と仮定する．この時 $\lambda\neq 0, -1$ にとれる．$\lambda g=g_t$ ならば

$$g_{st}=g_s g_t=(1+\lambda)g$$

となる．よって g_t と g_{st} の階数が一致するから (7.21) (iii) により st と t とは共役である．ところで G_0 による商群は可換だから $G_0st=G_0t$，すなわち $s\in G_0$ を得る．したがって $G_0=HG_0=O(Q)$ が成り立つ．

最後に $|F|=2$ の場合を考える．2次形式 Q の指数は極大全等方的部分空間の次元である．したがって指数が0または1ならば $g_s=0$ となる．(7.21) (ii) により $H=\{1\}$ を得るから $G_0=O(Q)$ となり定理が成り立つ．そこで Q の指数は少なくとも2と仮定する． 任意の交代形式は階数2の形式の和だから g_s の階数が2の場合に $s\in G_0$ を証明すればよい． この場合 P の中に一次独立な2元 y_1, y_2，N の中に一次独立な2元 x_1, x_2 があって

$$sy_1=y_1-x_2, \quad sy_2=y_2+x_1$$

をみたしている ((7.21) (iii) の証明参照)．部分空間 $\langle x_1, x_2, y_1, y_2\rangle$ を X とおけば X は非等方的で例外の場合を除けば $X^{\perp}\neq\{0\}$ となる．いま

$$U=\langle X^{\perp}, x_1, x_2\rangle$$

とおけば s は U の各元を不変にしている． X と共に $X^{\perp}$ も非等方的だから $X^{\perp}$ は非特異な元 z を含んでいる (7.6)．さて

$$z_1=z, \quad z_2=z+x_1+x_2, \quad z_3=z+x_2, \quad z_4=z+x_1$$

とおけば z_i は非特異である．そこで $\langle z_i\rangle^{\perp}$ に関する対称変換を s_i とおき

$$t=s_1s_2s_3s_4$$

と定義すれば t は G_0 の元である． ここで t が U の各元を不変にすることを示そう．U の元 u が $f(z, u)=0$ をみたせば $s_i(u)=u$ がすべての i について成り立つ．よって $t(u)=u$ を得る．一方，$f(z, u)\neq 0$ ならば

$$s_i(u)=u+z_i \qquad (i=1, 2, 3, 4)$$

となる．$f(z, z_i)=0$ だから $t(u)=u+z_1+z_2+z_3+z_4=u$ が成り立つ． よって t は U の各元を不変にする．計算を実行すれば

$$t(y_1)=y_1+x_2, \quad t(y_2)=y_2+x_1$$

となることがわかる．したがって $s=t\in G_0$ を得る． ▯

注意 定理 7.18 の例外の場合 G_0 は $O(Q)$ の指数 2 の部分群である．上定理の証明が難しいのは標数 2 の場合も含めたからである． ▯

§8 クリフォード環

直交群の構造を調べるために 2 次形式に対応するクリフォード環を定義する．この節では線形空間 V 上のテンソル代数 $T(V)$ の性質は既知のことと仮定するが一応定義と重要な性質をまとめておこう（『代数』 II, p. 325 参照）．

さて $T^0(V)=F, T^p(V)=V\otimes_F T^{p-1}(V)$ とおいて非負整数 p 全体にわたる直和 $T(V)=\sum T^p(V)$ が**テンソル代数**である． 2 元 $u\in T^p(V), v\in T^q(V)$ の積は $u\otimes v\in T^{p+q}(V)$ で与えられる．テンソル代数の中の積はこれを自然に拡張したものである．明らかに V と $T^1(V)$ とは同形であるから $T^1(V)$ をテンソル代数の部分空間とみて写像 $i: V\to T(V)$ が定義される． この時 $T(V)$ と i とは次の性質をもっている．

体 F 上の多元環 A と線形写像 $f: V\to A$ が与えられれば $\varphi\circ i=f$ をみたす F 多元環としての準同形 $\varphi: T(V)\to A$ が一意的に定まる．

この時 $\varphi(u_1\otimes\cdots\otimes u_p)=f(u_1)\cdots f(u_p)$ ($u_i\in V$, 右辺は多元環 A の中での積) となるから V を $T(V)$ の部分空間 ($T^1(V)=V$) と考えれば φ は f をテンソル代数の上に拡張したものとみることができる．

定義 8.1 線形空間 V 上で定義された 2 次形式を Q, それに同伴する形式を f とおく． V 上のテンソル代数を $T(V)$ とし，その中で

$$x\otimes x-Q(x)\cdot 1 \qquad (x\in V)$$

という形の元が生成する両側イデアルを $I(Q)$ とおく．商環 $T(V)/I(Q)$ を 2 次形式 Q の **Clifford 環**（略して C 環）といい，$C(Q)$ と表わす． ▯

以下 $u, v\in C(Q)$ の積は uv と単に並べて書くことにする． V から $T(V)$ の中への写像 i と $T(V)$ から $C(Q)$ の上への自然準同形を合成して

$$\rho=\rho_Q: V\longrightarrow C(Q)$$

が定まる．これが単射であることは後で証明する．定義から明らかに $C(Q)$ は V の元の ρ による像で生成されている．また任意の $x, y\in V$ について

(8.2) $$\rho(x)^2=Q(x)\cdot 1,\quad \rho(x)\rho(y)+\rho(y)\rho(x)=f(x,y)\cdot 1$$

が成り立つ.

定理 8.3 2次形式 Q のC環 $C(Q)$ と写像 $\rho_Q: V\to C(Q)$ は次の性質をもつ. いま F 多元環 A と線形写像 $h: V\to A$ が与えられ $h(x)^2=Q(x)\cdot 1$ がすべての $x\in V$ について成り立っていれば $g\circ\rho_Q=h$ をみたす F 多元環としての準同形 $g: C(Q)\to A$ が一意的に存在する.

証明 F 多元環 A と写像 h が与えられ上の条件をみたすと仮定する. 写像 h は一意的にテンソル代数 $T(V)$ に拡張される. その拡張を h' とおけば

$$h'(x\otimes x-Q(x)\cdot 1)=h(x)^2-Q(x)\cdot 1=0 \qquad (x\in V)$$

が成り立つ. よって h' の核はイデアル $I(Q)$ を含む. 準同形定理により h' は $T(V)/I(Q)=C(Q)$ から A の中への F 多元環準同形 g を定める. よって $g\circ\rho_Q=h$ を得る. $\rho_Q(V)$ が $C(Q)$ を生成するから g は一意的に定まる. □

系 組 $(C(Q),\rho_Q)$ は定理 8.3 の性質により一意的に定まる.

証明 上述の性質は普遍写像性だから $(C(Q),\ \rho_Q)$ が一意的に定まることはよく知られている(『代数』 II, p. 372 定理 1). □

あとで係数体の拡大をする時, 次の補題が必要となる.

(8.4) 体 F 上で定義された2次形式を Q とする. いま F の拡大体 E をとり, $U=E\otimes_F V$ とおく. すべての $x\in V$ について

$$Q'(1\otimes x)=Q(x)$$

をみたす U 上の2次形式 Q' が一意的に存在する. この時

$$C(Q')\cong E\otimes_F C(Q)$$

で $j(1\otimes\rho_Q(x))=\rho_{Q'}(1\otimes x)$ をみたす同形写像 j が一意的に定まる.

証明 V の F 基 $\{x_i\}$ をとれば $\{1\otimes x_i\}$ が U の E 基となる. したがって上式をみたす2次形式 Q' は一意的に定まる((7.3)参照). 逆に $\alpha_i\in E$ から

$$Q'(\sum_i \alpha_i\otimes x_i)=\sum_i \alpha_i{}^2 Q(x_i)+\sum_{i<j}\alpha_i\alpha_j f(x_i,x_j)$$

と Q' を定義すれば Q' は (8.4) の条件をみたす2次形式となる.

後半を証明するには $C'=E\otimes_F C(Q)$ とおいて $(C',1\otimes\rho_Q)$ が定理 8.3 の条件を満足することを示せばよい. E 多元環 A' と E 線形写像 $h': U\to A'$ が与えられ $h'(u)^2=Q'(u)\cdot 1$ が U の任意の元 u について成り立つとする. 写像 $g: x\longmapsto h'(1\otimes x)$ は

$$g(x)^2=h'(1\otimes x)^2=Q'(1\otimes x)\cdot 1=Q(x)\cdot 1$$

をみたす．したがって $g'\circ\rho_Q=g$ をみたす F 多元環準同形 $g':C(Q)\to A'$ が存在する(定理 8.3)．それは $C'=E\otimes_F C(Q)$ から A' の中への E 多元環準同形 h に拡張できる．この時 V の任意の元 x について

$$h(1\otimes\rho_Q(x))=g'(\rho_Q(x))=h'(1\otimes x)$$

となる．よって任意の $u\in U$ について $h((1\otimes\rho_Q)u)=h'(u)$ が成り立つ．すなわち $h\circ(1\otimes\rho_Q)=h'$ を得る．明らかにこの式をみたす写像 h は一意的に定まる．これは $(C', 1\otimes\rho_Q)$ が定理 8.3 の性質を満足していることを示している．定理 8.3 系により (8.4) が成り立つ． ▯

注意 2次形式 Q が恒等的に 0 の場合 Q の C 環は V 上の外積代数に他ならない．V の次元が n ならば V 上の外積代数の次元は 2^n である(『代数』 II，p. 329 定理 2)．このことは任意の 2 次形式 Q の C 環の場合にも成り立つ．ここでは外積代数の場合も含めて一緒に証明しよう．証明の途中で V の双対空間上の外積代数 $E(V^*)$ を用いるが，必要となる $E(V^*)$ の性質は(それがC環であるから)定理 8.3 に含まれている．なお $E(V^*)$ の 2 元 u, v の積は $u\wedge v$ と表わすことにする． ▯

(8.5) V の双対空間 V^* の元 f に対して次の性質(8.6)を満足する $T(V)$ の線形写像 i_f が一意的に定まる．

(8.6) $$i_f(1)=0,\quad i_f(x\otimes u)=f(x)u-x\otimes i_f(u),$$

ここで $x\in V, u\in T(V)$ である．この写像 i_f は $(i_f)^2=0$ をみたす．また $f\longmapsto i_f$ は V^* から $\mathrm{End}(T(V))$ の中への線形写像である．任意の 2 次形式 Q に対し i_f は両側イデアル $I(Q)$ を不変にしC環 $C(Q)$ の上の線形写像を引きおこす．

証明 (8.6)の第 1 式より i_f は $T^0(V)$ に一意的に定義される．そこで i_f が既に $T^p(V)$ 上で定義されたと仮定する．$T^p(V)$ の生成元の一つ u をとって(8.6)の第 2 式を用いれば $T^{p+1}(V)$ の生成元の一つ $x\otimes u$ に対する i_f の値が一意的に定まる．したがって i_f が $T(V)$ の上で一意的に定義される．このように定義された i_f が逆に (8.6) をみたしていることはすぐ検証される．

(8.6) の第 2 式に i_f を今一度適用すれば (i_f が線形写像だから)

$$(i_f)^2(x\otimes u)=x\otimes(i_f)^2(u)$$

を得る．第 1 式から $(i_f)^2$ は $T^0(V)$ の上で 0 となるから帰納法により $(i_f)^2$ はすべての p について $T^p(V)$ 上で 0 となる．したがって $(i_f)^2=0$ が成り立つ．

任意に $h, g\in V^*$ と $a, b\in F$ をとり $f=ag+bh$ とおく．この時 ai_g+bi_h は (8.6) の両式を満足している．よって i_f の一意性により

$$i_f=ai_g+bi_h.$$

2次形式 Q を定め $I=\{u\in I(Q)\mid i_f(u)\in I(Q)\}$ とおく．(8.6)の第2式により I は左イデアルとなる．ところで $I(Q)$ は左イデアルとして

$$u=(x\otimes x-Q(x)\cdot 1)\otimes v \qquad (x\in V, v\in T(V))$$

という形の元で生成されている．そこで $i_f(u)$ を計算してみれば

$$\begin{aligned} i_f(u)&=f(x)x\otimes v-x\otimes i_f(x\otimes v)-Q(x)i_f(v)\\ &=(x\otimes x-Q(x)\cdot 1)i_f(v)\in I(Q) \end{aligned}$$

となるから $I=I(Q)$，すなわち $i_f(I(Q))\subset I(Q)$ となる．i_f が $C(Q)$ に線形写像を引きおこしていることは明らかである． ▯

注意 いま $x_i\in V$ ならば $i_f(x_1\otimes x_2\otimes\cdots\otimes x_p)$ は

$$\sum(-1)^k f(x_k)(x_1\otimes\cdots\otimes\hat{x}_k\otimes\cdots\otimes x_p)$$

となる．ここで和記号の中の項は x_k を除いた残りの元のテンソル積である．

V の基 $\{u_i\}$ をとれば $\{u_i\otimes\cdots\otimes u_k\}$ が $T(V)$ の基となっている．V^* に双対基をとり，その1元 $d=d_j$ に対応する写像 i_d がどのように作用しているか調べてみよう．必要となるのは添数の集合 $J=\{i,\cdots,k\}$ が同じ文字を2重に含まない場合である．この時 $j\in J$ ならば

$$i_d(u_i\otimes\cdots\otimes u_k)=\pm u_i\otimes\cdots\otimes\hat{u}_j\otimes\cdots\otimes u_k$$

(右辺は u_j だけを除いた残りの元の積)，$j\notin J$ なら0である． ▯

2次形式 Q のC環を $C(Q)$ とする．任意の元 $g\in V^*$ に対してテンソル代数 $T(V)$ の線形写像 i_g が定まる (8.5)．そこで i_g が $C(Q)$ に引きおこす写像を $i(g)$ と表わす．いま $C(Q)$ 上の線形写像全体のつくる集合を L とおけば，L は F 上の多元環である．写像 $g\longmapsto i(g)$ は V^* から L の中への線形写像であるから定理8.3(恒等的に0となる2次形式の場合)により i は V^* 上の外積代数 $E(V^*)$ から L の中への多元環準同形 (同じ文字 i を用いて表わす) に拡張され $i(x\wedge y\wedge\cdots\wedge z)=i(x)i(y)\cdots i(z)$ が成り立つ．

線形空間 V の基 $\{u_1,\cdots,u_n\}$ を一つ定めておく．まだ $\rho=\rho_Q$ が単射であることは証明されていないが記号を簡単にするため $\rho(x)$ の代りに単に x と略記する．$C(Q)$ の元は $u_iu_j\cdots u_k$ という形の元の一次結合として表わされる．しかし添数を $i<j<\cdots<k$ と整理した元だけ用いればよい ((8.2)参照)．以上の

準備の下で次の定理が証明される．

定理 8.7 2次形式 Q のC環 $C(Q)$ の次元は 2^n である($n=\dim V$).

証明 上のように V の基 $\{u_1, \cdots, u_n\}$ を定めておく．$C(Q)$ の元

$$\{u_i u_j \cdots u_k \ (i<j<\cdots<k)\}$$

が一次独立であることを証明すればよい．そこで一次関係

$$(*) \qquad \sum a_{ij\cdots k} u_i u_j \cdots u_k = 0 \qquad (a_{ij\cdots k} \in F)$$

から $a_{ij\cdots k}=0$ を導こう．0でない係数があると仮定し，それらの項のうち添数の集合 J が最大となる項を一つとり $J=\{j, \cdots, k\}$ とおく．V^* に双対基 $\{d_i\}$ をとり $i(d_j \wedge \cdots \wedge d_k)$（添数の集合が J）による式（$*$）の像を考える．前に注意したように $i(d_j \wedge \cdots \wedge d_k)=i(d_j)\cdots i(d_k)$ は添数の集合が J の元 $u_j \cdots u_k$ 以外の各項を0にし，$u_j \cdots u_k$ を ± 1 に写す．よって（$*$）式から $\pm a_{ij\cdots k}=0$ となり矛盾が得られる．▯

系 1 写像 $\rho_Q : V \to C(Q)$ は単射である．

系 2 V の基 $\{u_1, \cdots, u_n\}$ を定めれば $\{u_j \cdots u_k \ (j<\cdots<k)\}$ がC環 $C(Q)$ の基となる．

証明 定理 8.7の証明から系2の成り立つことがわかる．系1は系2の特別の場合である．▯

定理 8.8 偶数次元 $n=2m$ の空間 V で定義された指数 m の非退化2次形式を Q とする．Q のC環は 2^m 次元の線形空間の自己準同形環と同形である．すなわちC環は $2^m \times 2^m$ 行列全体のつくる全行列環と同形である．

証明 仮定により V は二つの全特異部分空間 N と P との直和になる．ここで N も P も m 次元である．$V \subset C(Q)$ と考えて N から生成される部分環を S とおく．2次形式 Q の N 上への制限は恒等的に0だから S は N 上の外積代数と同形でその次元は 2^m である(定理 8.7)．そこで線形空間 S 上の線形写像全体がつくる多元環を L とおき $C(Q)$ と L とが同形になることを証明しよう．

2次形式 Q の同伴形式を f とおく．N に基 $\{x_1, x_2, \cdots, x_m\}$ を定め P の基 $\{y_1, \cdots, y_m\}$ を $f(x_i, y_j)=\delta_{ij}$ ($\delta_{ii}=1, \delta_{ij}=0 \ (i \neq j)$) となるようにとる．$P$ の元 y に対し $x \longmapsto f(x, y)$ は N^* の元である．補題 (8.5) によりこの N^* の元に対して S の線形写像が定義される．それを $i(y)$ とおく．(8.6) により任意の $x \in N$ と $u \in S$ について等式

$$i(y)xu=f(x,y)u-x(i(y)u)$$

が成り立つ．さて $u\longmapsto xu$ を $e(x)$ とおけば $e(x)$ は S の線形写像である．任意の $v\in V$ は $v=x+y$ $(x\in N, y\in P)$ と一意的に書ける．そこで

$$s(v)=e(x)+i(y)$$

とおけば s は V から L の中への線形写像で $(e(x)^2=i(y)^2=0)$

$$s(v)^2=e(x)i(y)+i(y)e(x)=f(x,y)=Q(v)\cdot 1$$

が成り立つ．（ここで $Q(x)=Q(y)=0$ も用いた．二つ目の等号は6行前の式による．）定理8.3により s を $C(Q)$ から L の中への多元環準同形に拡張できる．その拡張も同一文字 s で表わすことにする．定理8.7により

$$\dim C(Q)=2^{2m}=(\dim S)^2=\dim L$$

を得る．したがって準同形 s が全射であることを示せば $C(Q)\cong L$ となる．

さて $I=\{1,2,\cdots,m\}$ とおきその部分集合 H について $x_H=\prod x_i$ とおく．ここで積は H の元 i を増加順にかけたものである．定理8.7系2から $\{x_H\}$ が S の基となることがわかる．任意の $H\subset I, K\subset I$ に対し

$$v_{H,K}=x_H y_I x_{I-K} \qquad (y_I=y_1y_2\cdots y_m)$$

とおき $\{s(v_{H,K})\}$ が L を生成することを証明しよう．基 $\{y_i\}$ は N の基 $\{x_i\}$ の双対基にあたるから前に注意したように $j\notin H$ ならば

$$s(y_j)x_H=i(y_j)x_H=0, \quad s(y_j)x_jx_H=x_H$$

が成り立つ．N の元の自乗は0だから $H\cap K\neq\varnothing$ ならば $x_Hx_K=0$．したがって

$$s(v_{H,K})x_L=\begin{cases}0 & (K\neq L)\\ \pm x_H & (K=L)\end{cases}$$

となる．よって $s(v_{H,K})$ の全体は L を生成する． □

注意 $\dim C(Q)=\dim L$ だから上の全射準同形 s は単射である．よく知られているように体上の全行列環は単純環でその中心は係数体 F と一致する．定理8.8の仮定の下でC環 $C(Q)$ はいわゆる中心的単純環である． □

定理 8.9 偶数次元の空間で定義された非退化2次形式を Q とする．Q の指数にかかわらず Q のC環 $C(Q)$ は中心的単純環である．

証明 係数体 F の代数的閉包を E とおく．Q に対応して $E\otimes_F V$ 上に

$$Q'(1\otimes x)=Q(x)$$

をみたす2次形式Q'が定まる(8.4)．この時Q'に同伴する形式f'はQの同伴形式を $E\otimes V$ に拡張したものだからf'は非退化である(I§4参照)．前に注意したように代数的閉体の上では非退化2次形式は極大指数をもつから定理8.8により $C(Q')$ は全行列環に同形で中心的単純環である(『代数』II, p.317例2)．一方，(8.4) により $C(Q')\cong E\otimes_F C(Q)$ が成り立つ．このことから $C(Q)$ も中心的単純環になる(『代数』II, p.319補題2, p.418補題4)． □

テンソル代数 $T(V)$ においてpを偶数だけに限った和 $\sum T^p(V)$ を T^+, 奇数だけの和をT^-とおく．明らかに線形空間として $T(V)$ はT^+とT^-との直和となる．このことからC環 $C(Q)$ もT^+の像C^+とT^-の像C^-の直和に分解することがわかる．T^+は $T(V)$ の部分環だからC^+は $C(Q)$ の部分環である．さらに $C^+C^-\subset C^-, C^-C^+\subset C^-, C^-C^-\subset C^+$ が成り立つ．

定理 8.10　偶数次元の空間で定義された非退化2次形式をQとする．この時C^+は半単純で，C^+の中心ZはF上2次元である．Zが体ならばZはFの分離拡大体でC^+は単純環，Zが体でなければC^+は二つの単純環の直和である．

証明　まずQは極大指数の2次形式であると仮定する．定理8.8の証明に用いた記号を用い $S^+=S\cap C^+, S^-=S\cap C^-$ とおけば $\{x_H\,|\,|H|$ は偶数$\}$ が S^+ の基となる．よってSはS^+とS^-との直和に分解する．任意の $x\in N$ について $e(x)$ はS^+とS^-とを交換する．これは $i(y)$ $(y\in P)$ についても同様である．したがって任意の $v\in V$ について $s(v)$ はS^+とS^-とを入れ替えるから $s(C^+)$ の各元はS^+もS^-も不変にしている．そこで S^+, S^- 上の線形写像全体のつくる多元環をそれぞれ L^+, L^- とおけばsはC^+からL^+とL^-との直和の中への単射準同形を与える．ところでF上の次元が

$$\dim C^+=2^{n-1}=2(2^{m-1})^2=\dim L^++\dim L^- \qquad (n=2m)$$

をみたしているから $s(C^+)=L^++L^-$ すなわちC^+は二つの $2^{m-1}\times 2^{m-1}$ 全行列環の直和である．

指数が任意の場合は前定理の証明のようにFの代数的閉包Eをとり，QをE上の2次形式Q'に拡張する．この時 $C^+(Q')=E\otimes_F C^+(Q)$ が成り立つ．よって $C^+(Q)$ の中心ZはF上2次元である．さて $C^+(Q)$ の根基をRとおけば，Rはベキ零だから $E\otimes R$ は $C^+(Q')$ のベキ零イデアルとなる．ところで

$C^+(Q')$ は単純環の直和だから半単純で $E\otimes R=\{0\}$，すなわち $R=\{0\}$ で $C^+(Q')$ は半単純である(『代数』 I，第2章§9参照)．中心 Z が体の場合，Z が F の分離拡大体であることはテンソル積 $E\otimes Z$ が体の直和になることから証明される．(『代数』 II，p. 321 定理2の前の注意参照.）残っている点は半単純環の構造定理から明らかである． □

定理 8.11 奇数次元の空間で定義された非退化2次形式を Q とおく．$C^+(Q)$ は中心的単純環である．$C(Q)$ の中心を Z とおけば Z は F 上2次元で

$$C(Q)\cong Z\otimes_F C^+(Q)$$

が成り立つ．また Z は C^- の可逆元を含む．

証明 非特異元 x_0 をとり $U=\langle x_0\rangle^\perp$ とおく．U の元 u に

$$Q_1(u)=-Q(x_0)Q(u)$$

を対応させれば U 上に非退化2次形式 Q_1 が得られる．さて $u\longmapsto x_0u$ は U から $C^+(Q)$ の中への線形写像で（$f(x_0,u)=x_0u+ux_0=0$ より）

$$(x_0u)^2=x_0ux_0u=-x_0{}^2u^2=-Q(x_0)Q(u)=Q_1(u)$$

が成り立つ．定理 8.3 によりこの写像をC環 $C(Q_1)$ から $C^+(Q)$ の中への多元環準同形 h に拡張できる．定理 8.9 により $C(Q_1)$ は単純であるから h は単射となる．（$h(1)=1$ より $h\neq 0$.）ところで $C(Q_1)$ と $C^+(Q)$ とは F 上同次元であるから h は全射となる．よって $C(Q_1)\cong C^+(Q)$ が成り立ち $C^+(Q)$ は中心的単純環である．

次に U の直交基 $\{x_1,\cdots,x_{2m}\}$ をとり $z=x_0x_1\cdots x_{2m}$ とおく．任意の i,j について $x_ix_j=-x_jx_i$ が成り立つから $x_iz=(-1)^{2m}zx_i=zx_i$ となり z は中心 Z の元である．また $z^2=\pm Q(x_0)Q(x_1)\cdots Q(x_{2m})$ だから z は中心の可逆元で明らかに C^- に属する．よって $Z_0=F\cdot 1+Fz$ は部分環で

$$Z_0\otimes_F C^+(Q)\longrightarrow C(Q)$$

は多元環準同形である．$z\notin C^+(Q)$ だから $Z_0\otimes_F C^+(Q)=C(Q)$ となり Z_0 は $C(Q)$ の中心 Z と一致する． □

最後にC環の**主反自己同形** β について述べる．任意の多元環 A の**反自己同形**とは A の線形写像 α であって，α は可逆，$\alpha(1)=1$，かつ積について

$$\alpha(ab)=\alpha(b)\alpha(a) \qquad (a,b\in A)$$

が成り立つものである(右辺と左辺で a,b の順序が逆)．

定理 8.12 空間 V 上で定義された2次形式を Q，そのC環を $C(Q)$ とする．この時 $C(Q)$ の反自己同形 β で各 $x\in V$ について $\beta(x)=x$ をみたすものが一意的に存在する．

証明 この様な β が存在すると仮定すれば任意の $x_i\in V$ について

$$\beta(x_1x_2\cdots x_r)=x_r\cdots x_2x_1 \qquad (\text{右辺の積は逆順})$$

が成り立つから β が一意的に定まることは明らかである．β が存在することは次のように証明される．$C(Q)$ と反同形な多元環を C' とおけば V から C' の中への線形写像 s がある．任意の $x\in V$ について $x^2=Q(x)\cdot 1$ が成り立つから定理 8.3 により s は $C(Q)$ から C' の中への多元環準同形に拡張できる．この準同形も同じ文字 s で表わす．$s(V)$ が C' の生成集合だから s は全射である．一方 $C(Q)$ と C' とは同次元だから s は単射で実は同形写像である．そこで C' から $C(Q)$ の上への反同形写像との合成を β とおけば，β は $C(Q)$ の反自己同形で条件 $\beta(x)=x$ $(x\in V)$ を満足する． ▯

定義 8.13 上定理の β をC環 $C(Q)$ の**主反自己同形**という．

§9 直交群の交換子群

この節では空間 V で定義された2次形式 Q は非退化と仮定する．直交群の交換子群を決定するのが目標である．その基本となる Q に対応するC群という概念を定義する．

定義 9.1 2次形式 Q のC環を $C(Q)$ とし，V を $C(Q)$ の部分空間と考える．2次形式 Q の **Clifford 群**（略してC群）というのは $C(Q)$ の可逆元 s で条件 $sVs^{-1}=V$ を満足するもの全体がつくる群である． ▯

定理 9.2 2次形式 Q のC群を G とおき，$G^+=G\cap C^+$，また

$$\varphi(s)x=sxs^{-1} \qquad (s\in G,\ x\in V)$$

とおく．この時，次の命題が成り立つ．

(i) 写像 φ は G から直交群 $O(Q)$ の中への準同形でその核は $C(Q)$ の中心に含まれる可逆元全体の集合と一致する．

(ii) 集合 $V\cap G$ は V の非特異元の全体と一致し，任意の $x\in V\cap G$ について $-\varphi(x)$ は超平面 $\langle x\rangle^\perp$ に関する対称変換である．

(iii) V の次元が偶数の場合，G の各元は C^+ の元であるかまたは C^- の元で

ある．$V \neq \{0\}$ ならば G^+ は指数 2 の部分群である．

(iv)　空間 V が偶数次元の場合 $\varphi(G)=O(G)$ である．さらに $V \neq \{0\}$ ならば $\varphi(G \cap C^-) \cap \varphi(G^+)=\varnothing$ で $\varphi(G^+)$ は $O(G)$ の指数 2 の部分群となる．係数体の標数が 2 でなければ $\varphi(G^+)$ は $SO(Q)$ と一致する．

(v)　V の次元が奇数の場合は $\varphi(G)=\varphi(G^+)=SO(Q)$ となる．

証明　(i)　任意の $s \in G$ と $x \in V$ について $C(Q)$ の中で

$$Q(\varphi(s)x)=(sxs^{-1})^2=sx^2s^{-1}=Q(x)$$

が成り立つ．したがって $s \in G$ ならば $\varphi(s) \in O(Q)$ が成り立つ．写像 φ が準同形であること，すなわち $\varphi(st)=\varphi(s)\varphi(t)$ が成り立つことは定義から容易に証明される．いま $s \in G$ に対し $\varphi(s)=1$ であると仮定すれば s はすべての V の元と可換になる．$C(Q)$ は V の元で生成されるから s は $C(Q)$ の中心の元である．よって (i) が証明された．

(ii)　V の一元を x とすれば $x^2=Q(x)$ が成り立つから x が可逆元であるための条件は $Q(x) \neq 0$，すなわち x が非特異な元であることである．この時 x の逆元は $Q(x)^{-1}x$ であるから，任意の $y \in V$ について

$$\begin{aligned} xyx^{-1}&=Q(x)^{-1}xyx=Q(x)^{-1}x(f(x,y)-xy) \\ &=-y+Q(x)^{-1}f(x,y)x \end{aligned}$$

が成り立つ((8.2)参照)．したがって V の元 x が非特異ならば x はC群の元で $-\varphi(x)$ は $\langle x \rangle^\perp$ に関する対称変換である(定義 7.15)．

(iii)　空間 V の次元が偶数ならば Q のC環 $C(Q)$ は中心的単純環である(定理 8.9)．定義により $sx=\varphi(s)xs$ が任意の $x \in V$ について成り立つ．そこで $s=t+r$ $(t \in C^+, r \in C^-)$ とおけば sx の C^- 成分は tx である．また $\varphi(s)xs$ の C^- 成分は $\varphi(s)xt$ だから $tx=\varphi(s)xt$ となる．したがって

$$s^{-1}tx=s^{-1}\varphi(s)xt=xs^{-1}t$$

がすべての $x \in V$ について成り立つ．これは $s^{-1}t$ が $C(Q)$ の中心 Z に含まれることを示している．ところで $C(Q)$ は中心的単純環だから $t=as$ $(a \in F)$ となる．もし $a \neq 0$ ならば $s=a^{-1}t \in C^+$．これに反し $a=0$ ならば $s=r \in C^-$ となる．いま $V \neq \{0\}$ ならば V は非特異元 x を含む(7.6)．(ii)の証明のはじめに述べたように x は可逆元で $x \in G \cap C^-$，また $(G \cap C^-)x \subset G^+$ が成り立つ．したがって G^+ は G の指数 2 の部分群である．

(iv)　$O(Q)$ の任意の元 u をとる．この時 u は V から $V\subset C(Q)$ への線形写像で $u(x)^2=Q(u(x))=Q(x)$ が成り立つ．よって定理 8.3 により u を $C(Q)$ から $C(Q)$ の中への多元環準同形に拡張できる．ところで $C(Q)$ は単純環で u は V 上で 0 でないから u は $C(Q)$ の自己同形に拡張できる．この拡張は係数体 F の元を不変にするから，単純環の一定理（『代数』 II, p. 422 系 3）により u は $C(Q)$ の内部自己同形に拡張される．すなわち $C(Q)$ の可逆元 s があって

$$u(x)=sxs^{-1}$$

が V のすべての元 x について成り立つ．これは $s\in G$ かつ $u=\varphi(s)$ が成り立つことを示している．したがって $\varphi(G)=O(Q)$ が成り立つ．

$C(Q)$ の中心は F だから $\ker\varphi\subset G^+$ (i)．よって

$$\varphi(G\cap C^-)\cap\varphi(G^+)=\varnothing,\quad |\varphi(G):\varphi(G^+)|=|G:G^+|=2$$

が成り立つ．以下係数体 F の標数は 2 でないと仮定する．定理 7.18 により直交群 $O(Q)$ の元 u は対称変換の積となる．そこで非特異元 $x_1,\cdots,x_k$ があって u が $\langle x_i\rangle^\perp$ に関する対称変換の積であるとすれば (ii) により

$$u=(-1)^h\varphi(x_1\cdots x_h)$$

が成り立つ．対称変換の行列式の値は -1 だから $\det u=(-1)^h$ となる．したがって $u\in SO(Q)$ ならば h は偶数となり $u\in\varphi(G^+)$ が成り立つ．すなわち $SO(Q)\subset\varphi(G^+)$ であるが $SO(Q)$ も $\varphi(G^+)$ も $O(Q)$ の指数 2 の部分群だから $SO(Q)=\varphi(G^+)$ となる．

(v)　V が奇数次元の場合は係数体の標数は 2 でない．したがって上の証明がそのまま成り立ち $SO(Q)\subset\varphi(G^+)\subset\varphi(G)$ を得る．ところでこの場合 $\varphi(G)$ は $O(G)$ と一致しないことが次の様に証明される．$SO(Q)$ の指数が 2 だから $SO(Q)=\varphi(G^+)=\varphi(G)$ が成り立つ．

V の写像 $x\longmapsto -x$ は $O(Q)$ の元である．しかしこの元は $\varphi(G)$ に含まれていない．実際もしこの写像が $C(Q)$ の可逆元 t により引きおこされたと仮定すればすべての $x\in V$ について $txt^{-1}=-x$ が成り立つ．そうすれば任意の $v\in C^-$ について $tvt^{-1}=-v$ が成り立つはずである．ところが $C(Q)$ の中心は C^- の可逆元を含むから矛盾が得られる（定理 8.11 参照）．　□

次にスピンノルムを定義する．

(9.3)　非退化 2 次形式を Q，その C 環 $C(Q)$ の主反自己同形を β とする．

任意の $s\in G^+$ について $N(s)=\beta(s)s$ とおけば N は G^+ から F の中への準同形である.

証明 もし $s\in G^+$ ならば $sVs^{-1}=V$ が成り立つ. この式の β による像をとって $\beta(s)^{-1}V\beta(s)=V$ を得る. ゆえに $\beta(s)$ も G^+ の元である. さて任意の元 $x\in V$ に対して $sx=\varphi(s)xs$ が成り立つから

$$x\beta(s)=\beta(s)\varphi(s)x,$$

したがって $\beta(s)sx=\beta(s)\varphi(s)xs=x\beta(s)s$ が成り立つ. ここで x は V の任意の元だから $\beta(s)s$ は $C(Q)$ の中心 Z の元である. ところで前節で述べた $C(Q)$ の構造定理によれば (定理 8.9, 8.11) $Z\cap G^+$ は F の可逆元の集合と一致する. したがって $\beta(s)s\in F^*$ となる. β は反自己同形だから

$$\beta(st)st=\beta(t)\beta(s)st=\beta(s)s\beta(t)t$$

すなわち $N(st)=N(s)N(t)$ が任意の $s,t\in G^+$ について成り立つ. □

写像 φ は G^+ から $O(Q)$ の中への準同形を引きおこし, その核は F^* と一致する. そこで $\varphi(G^+)$ の任意の元 σ に対し $\varphi(u)=\sigma$ となる G^+ の元 u は F^* の元を除いて一意的に定まる. もし $a\in F^*$ ならば $N(a)=a^2$ であるから $N(u)$ は F^* の元の自乗を除いて一意的に定まる. すなわち

$$\nu:\sigma\longmapsto N(u)\qquad(\varphi(u)=\sigma)$$

は $\varphi(G^+)$ から $F^*/(F^*)^2$ の中への準同形を与える.

定義 9.4 (9.3)で定義した $N(s)$ を G^+ の元 s の**スピンノルム**という. 本書では $\nu(\sigma)$ も $\varphi(G^+)$ の元 σ のスピンノルムという. N の核を G_0^+ とおき**被約C群**という. □

商群 $\varphi(G^+)/\varphi(G_0^+)$ の構造を調べるため次の補題を証明しよう.

(9.5) 一つの例外(2元体上の4次元空間で定義された指数2の2次形式)を除けば G^+ の元は偶数個の $V\cap G$ の元の積となる.

証明 上の例外の場合を除けば任意の直交変換は対称変換の積となる (定理 7.18). G^+ の元 s をとり $\varphi(s)=\tau_1\cdots\tau_h$ と対称変換 τ_i の積として書く. 各 τ_i は非特異元 x_i と直交する超平面に関する対称変換とすれば定理 9.2 により $\varphi(s)=(-1)^h\varphi(x_1\cdots x_h)$ となる. ここで $(-1)^h=1$ が成り立つ. 係数体の標数が2であればこれは自明であるし, 標数$\neq 2$ の場合は $\varphi(G^+)=SO(Q)$ だから h が偶数となるからである. したがって $\varphi(s)=\varphi(x_1\cdots x_h)$ が成り立つ. そこで

$s=cx_1\cdots x_h$ とおけば c は φ の核に含まれている．ここで $c\in F$ となることを証明しよう．定理 9.2(i) により φ の核は $C(Q)$ の中心に含まれる．偶数次元の場合 $C(Q)$ は中心的単純環だから $c\in F$ が成り立つ(定理 8.9)．奇数次元の場合は $\varphi(G^+)=SO(Q)$ だから h が偶数となり（定理 8.11 より）

$$c\in Z\cap C^+=F$$

が成り立つ．よって $s=(cx_1)x_2\cdots x_h$ と $V\cap G$ の元の積となる．$s\in G^+$ だから(標数 2 の場合でも) h は偶数である． □

(9.6) 体 F の乗法群 F^* の中で積 $Q(x)Q(y)$ $(x, y\in V\cap G)$ が生成する部分群を H とおく．もし $V\neq\{0\}$ ならば ν の核は $\varphi(G_0^+)$ で

$$\varphi(G^+)/\varphi(G_0^+)\cong H/(F^*)^2$$

が成り立つ．2 次形式 Q の指数が正ならば $H=F^*$ である．いま $\varphi(G^+)$ の元 σ が対称変換 τ_i の積で，$\sigma=\tau_1\cdots\tau_h$，各 i について τ_i は非特異元 x_i と直交する超平面に関する対称変換であると仮定すれば次式が成り立つ．

$$\nu(\sigma)=Q(x_1)\cdots Q(x_h)(F^*)^2.$$

証明 係数体が 2 元体の場合は $G^+=G_0^+$, $F^*=(F^*)^2$ だから (9.6) が成り立つ．そこで $|F|>2$ と仮定する．G^+ の元 s は (9.5) により

$$s=x_1\cdots x_h \qquad (x_i\in V\cap G, h \text{ は偶数})$$

と書くことができる．$\beta(s)$ は逆順序の積 $x_h\cdots x_1$ となるから

$$N(s)=Q(x_1)\cdots Q(x_h)$$

が成り立つ．したがって ν による像は部分群 H と一致する(h が偶数)．さて ν の核の元 σ をとり $\varphi(u)=\sigma$ とすれば $N(u)$ は F^* の元の自乗となる．よって $N(cu)=1$ をみたす F^* の元 c がある．すなわち $cu\in G_0^+$，また

$$\varphi(cu)=\varphi(u)=\sigma$$

が成り立つ．これは ν の核が $\varphi(G_0^+)$ であることを示している．そこで ν により同形対応 $\varphi(G_0)/\varphi(G_0^+)\cong H/(F^*)^2$ が得られる．

さて Q の指数が正ならば強双曲型の組がある．したがって Q の値は F の任意の元をとり $H=F^*$ が成り立つ．最後の公式はいまや明らかである． □

以上の準備の下で本節の主定理が証明される．

定理 9.7 2 次形式 Q の指数は正と仮定し，さらに (9.5) であげた例外の場合ではないと仮定する．この時 $O(Q)$ の交換子群は $\varphi(G_0^+)$ である．

証明　$O(Q)$ の交換子群を Ω, また $\Phi=\varphi(G_0^+)$ とおく．

(a)　まず $\Omega\subset\Phi$ が成り立つことを証明しよう．Q の定義されている空間 V の次元が奇数か偶数かにより二つの場合に分ける．

dim V が奇数の場合　写像 $x\longmapsto -x$ $(x\in V)$ を ζ とおく．ζ は $O(Q)$ の中心に含まれているが $SO(Q)$ の元ではない．そこで $Z=\langle\zeta\rangle$ とおけば直積分解 $O(Q)=Z\times\varphi(G^+)$ が成り立つ (定理 9.2(v) 参照)．定義により Φ は $\varphi(G^+)$ の正規部分群だから $\Phi\lhd O(Q)$ となる．さらに

$$O(Q)/\Phi\cong Z\times(\varphi(G^+)/\Phi)$$

が成り立つから (9.6) により $O(Q)/\Phi$ は可換群である．よって $\Omega\subset\Phi$ となる．

dim V が偶数の場合　この場合，写像 N を G のすべての元について定義できる．この写像の核を G_0 とおく．さて Q の指数は正と仮定したからスピンノルムは G^+ から F^* の上への全射となる．したがって $G=G_0G^+, G_0\cap G^+=G_0^+$ が成り立ち $G_0^+\lhd G$ および $G/G_0^+\cong(G/G^+)\times(G^+/G_0^+)$ を得る．よって商群 G/G_0^+ は可換群である．定理 9.2 により $\varphi(G)=O(Q)$ となるから Φ は $O(Q)$ の正規部分群で $O(Q)/\Phi$ は可換群となる．よって $\Omega\subset\Phi$ を得る．

(b)　Q の指数は正と仮定したから V は強双曲型の組 $\{x, y\}$ を含んでいる．さて $P=\langle x, y\rangle$ とおき V を直交和 $P\oplus P^\perp$ に分解する．$O(Q)$ の元のうち $P^\perp$ の各元を不変にするもの全体の集合を H とおく．H は $O(Q)$ の部分群である．ここで $O(Q)=\Omega H$ が成り立つことを証明しよう．Ω は正規部分群だから ΩH は部分群である．したがって ΩH が対称変換をすべて含んでいることを証明すればよい (定理 7.18)．

任意の対称変換を σ とする．σ はある非特異元 z に直交する超平面 L に関する対称変換である．いま P の元 z_1 を $z_1=x+Q(z)y$ と定義すれば

$$Q(z_1)=Q(z)$$

が成り立つ．よって Witt の定理により z を z_1 にうつす $O(Q)$ の元 τ がある．そこで $\sigma_1=\tau\sigma\tau^{-1}$ とおけば σ_1 は τL に関する対称変換である．ところで $\tau(z)=z_1\in P$ だから $\tau L\supset P^\perp$ となり $\sigma_1\in H$ を得る．したがって

$$\sigma=\sigma\sigma_1^{-1}\sigma_1,\quad \sigma\sigma_1^{-1}=\sigma\tau\sigma^{-1}\tau^{-1}\in\Omega$$

が成り立ち $\sigma\in\Omega H$ が証明される．よって $O(Q)=\Omega H$ となる．

(c)　記号 $P=\langle x, y\rangle$ は (b) で定めた通りとする．任意の $a\in F^*$ に対して

$w_a=x+ay$ とおく．部分群 H も (b) の通りとする．ここで H の元は

$$-\varphi(w_a) \quad \text{または} \quad \varphi(w_a w_1)$$

と表わせることを示そう． H の元は P を全体として不変にする． P の特異元は二つの1次元部分空間 Fx と Fy のいずれかに含まれているから H の元は $P^\perp$ の各元を不変にして P の上では

$$\tau_a: \begin{array}{l} x \longrightarrow -ay \\ y \longrightarrow -a^{-1}x \end{array}, \quad \rho_a: \begin{array}{l} x \longrightarrow a^{-1}x \\ y \longrightarrow ay \end{array}$$

のいずれかに一致する．したがって H の元は $-\varphi(w_a)$ または $\varphi(w_a w_1)$ である．

(d) $\Phi\subset\Omega$ が成り立つことを証明しよう．そこで Φ の任意の元 σ をとる．(b) により $\sigma=\sigma_1\sigma_2$ $(\sigma_1\in\Omega, \sigma_2\in H)$ と書くことができる．(a) より $\Omega\subset\Phi$ を得るから $\sigma_2\in\Phi$ となる．ここで $\sigma_2=\varphi(w_a w_1)$ の形であることを示そう．(c) によれば σ_2 が $-\varphi(w_a)$ の形でないことをいえばよい．係数体の標数が2でなければ $-\varphi(w_a)$ の行列式の値は -1 だから σ_2 とは一致しない（Φ の元は $\varphi(G^+)=SO(Q)$ に含まれている）．一方，係数体の標数が2ならば V の次元は偶数である．よって定理9.2 (iv) により $\varphi(w_a)\notin\varphi(G^+)$ を得る．いずれの場合も σ_2 は $\varphi(w_a w_1)$ の形をしている．さて $\sigma_2\in\Phi$ だからスピンノルムが1，すなわち (9.6) により

$$Q(w_a)Q(w_1)=a\in(F^*)^2$$

を得る．そこで $a=b^2, \rho=\varphi(w_b w_1), \tau=-\varphi(w_1)$ とおけば

$$\sigma_2=\rho\tau\rho^{-1}\tau^{-1}\in\Omega$$

であることが容易に確かめられる．したがって $\sigma=\sigma_1\sigma_2\in\Omega$ となり $\Phi\subset\Omega$ が成り立つ．(a) と併せて $\Phi=\Omega$，すなわち定理が成り立つ． ∎

定理 9.8 前定理と同じ条件を仮定する．さらに $\dim V>2$ であると仮定すれば $\varphi(G_0^+)$ は $\varphi(G^+)$ の交換子群である．

証明 (a) 対称変換 σ, τ の交換子 $[\sigma, \tau]$ 全体が生成する部分群を K とおき $K=\Omega$ が成り立つことを証明しよう．ここで Ω は $O(Q)$ の交換子群である．さて $K\subset\Omega$ となることは明らかだから $\Omega\subset K$ を証明する．(7.17) により K は $O(Q)$ の正規部分群である．例外の場合は除いてあるから $O(Q)$ は対称変換の全体で生成されている．商群 $O(Q)/K$ は対称変換の像で生成されるがそ

れらの像は互いに交換可能である．よって $O(Q)/K$ は可換群となり K は交換子群 Ω を含む．したがって $K=\Omega$ が成り立つ．

(b)　対称変換 σ, τ の交換子 $[\sigma, \tau]$ が $\varphi(G^+)$ の交換子として書けることを証明する．そこで

$$\sigma=s_H, \quad \tau=s_L, \quad H^\perp=\langle x\rangle, \quad L^\perp=\langle y\rangle$$

とおく．場合を分けてまず $\langle x, y\rangle^\perp$ が全特異でない場合を考える．この時，非特異元 $z\in\langle x, y\rangle^\perp$ をとり $\langle z\rangle^\perp$ に関する対称変換を ρ とおけば ρ は σ とも τ とも可換である(7.16)．したがって

$$[\sigma, \tau]=[\sigma\rho, \tau\rho]$$

が成り立つ．さらに $\sigma\rho=\varphi(xz)\in\varphi(G^+)$，同様に $\tau\rho\in\varphi(G^+)$ となる．

(c)　残っているのは $\langle x, y\rangle^\perp$ が全特異の場合である．この時は

$$\langle x, y\rangle^\perp\subset\langle x, y\rangle^{\perp\perp}=\langle x, y\rangle$$

が成り立つ．ところで $\langle x, y\rangle^\perp$ の次元は少なくとも $n-2$ ($n=\dim V$) だから $n-2\leqq 2$ となる．元 x は非特異だからここで等号は成り立たない．仮定により $n>2$ だから上の不等式より $n=3$ を得る．この場合は

$$[\sigma, \tau]=[-\sigma, -\tau]$$

で $-\sigma, -\tau\in SO(Q)=\varphi(G^+)$ となる．　▯

注意　$n=2$ の場合 $\varphi(G^+)$ は可換群で定理 9.8 は成り立たない．　▯

第3章　Lie 型の単純群

§1　根　　系

1. 定義　有限次元 Euclid 空間を E とおき，E の2元 u, v の**内積**を単に (u, v) と表わす．0以外の任意の元 $r \in E$ に対し

(1.1)
$$w_r(x) = x - 2(r, x)(r, r)^{-1} r$$

により E の線形写像 w_r が定義される．いま原点を通り r に直交する元全体のつくる超平面を H とおけば w_r は H に関する対称変換である．この節では H より r を重視するから w_r を r に関する対称変換ともいう．以下の考察で重要となる根系という概念を定義しよう．

定義 1.2　次の条件をみたす E の部分集合 Δ を**根系**という．

(i)　Δ は有限集合で $0 \notin \Delta$.

(ii)　Δ の元が生成する部分空間は E と一致する．

(iii)　$r, s \in \Delta \Longrightarrow w_r(s) \in \Delta$.

(iv)　$r, s \in \Delta \Longrightarrow 2(r, s)/(s, s)$ は整数である．

(v)　$r \in \Delta, \lambda r \in \Delta$ $(\lambda \in \boldsymbol{R}) \Longrightarrow \lambda = \pm 1$.

根系 Δ の元 r を**根**といい，E の次元が l の時 Δ を l 次元の根系という．任意の $r \in \Delta, s \in \Delta$ に対して

$$n(r, s) = 2(r, s)/(s, s)$$

とおく．(条件 (iv) により $n(r, s)$ は整数である．) さらに

$$W(\Delta) = \langle w_r \mid r \in \Delta \rangle$$

とおき，$W(\Delta)$ を根系 Δ の **Weyl 群**という．□

注意　根系 Δ の元 r をとれば $w_r(r) = -r$ となる．したがって (iii) により $r \in \Delta \Rightarrow -r \in \Delta$ が成り立つ．また $W(\Delta)$ の各元は Δ を Δ の上にうつす．もし $W(\Delta)$ の元 w が Δ の各元を不変にすれば (ii) より $w = 1$ を得る．よって根系の Weyl 群は Δ の元の上の置換群と考えられ，特に $W(\Delta)$ は有限群である(i)．このことから $W(\Delta)$ は Coxeter 群となる(『群論』上 p. 354)．□

(1.3)　Δ を根系とし Δ の2元 r, s の間の角を θ とおく．この時 θ は

$$0°,\quad 30°,\quad 45°,\quad 60°,\quad 90°,\quad 120°,\quad 135°,\quad 150°,\quad 180°$$

のいずれかに等しい．そして $0 \leqq \theta < 90°$, $(r, r) \leqq (s, s)$ ならば $\theta = 30°, 45°, 60°$ に応じて $(s, s)/(r, r) = 3, 2, 1$ となる．

証明　衆知のように $\cos^2\theta = (r, s)^2/(r, r)(s, s)$ が成り立つ．よって

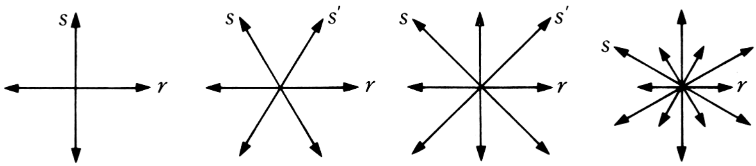
$$n(r, s)n(s, r) = 4\cos^2\theta \leqq 4$$

となる．ところでこの左辺は根系の条件(iv)により二つの整数の積である．このことから $\cos^2\theta = 0, 1/4, 1/2, 3/4$, または 1 となり θ が上にあげた値のいずれかに等しいことがわかる．また $0 < \theta < 90°$ と制限すれば

$$n(r, s) = 1, \quad n(s, r) = 1, 2, 3$$

となり後半が証明される．□

(1.4)　根系 Δ の 2 元 r, s をとり $s \neq \pm r$ と仮定する．2 元 r, s が生成する平面を P とし $\Delta_1 = \Delta \cap P$ とおけば Δ_1 は P に含まれる 2 次元の根系である．2 次元の根系は次の 4 通りに限る．



D_2　　A_2　　B_2　　G_2

証明　Δ_1 が根系であるための条件 (i)—(v) をみたしていることを示せばよいがそれは明らかであろう．2 次元の根系 Δ の中に 2 元 r, s を $s \neq -r$, さらに r と s との間の角 θ が最大になるように選ぶ．この時 $90° \leqq \theta < 180°$ となるから (1.3) により $\theta = 90°, 120°, 135°, 150°$ のいずれかである．各場合に Δ が一意的に定まる．例えば $\theta = 135°$ としよう．この時

$$w_r(s) = s', \quad w_s(r) = r'$$

とおけば s' も r' も Δ の元となる(条件(iii))．ところで $\pm r, \pm s, \pm r', \pm s'$ が中心角の 8 等分線上にのっているからこれらの元以外に Δ の元はない．よって Δ は B_2 型である．□

注意　根系の条件 (i)—(v) は強い条件ですべての次元で根系はすっかり分類されている．□

(1.5)　根系 Δ の 2 元 r, s をとり $s \neq \pm r$ と仮定する．もし $n(r, s) > 0$ なら

ば $r-s$ は根である．($n(r,s)>0 \Leftrightarrow (r,s)>0$ が成り立つ．)

証明　(1.4) を用い個別に (1.5) の成り立つことを確かめることができる．次の様に証明することもできる．(1.3) の証明からわかるようにこの補題の仮定の下で $n(r,s)=1$ または $n(s,r)=1$ が成り立つ．$n(r,s)=1$ なら

$$w_s(r)=r-n(r,s)s=r-s\in\Delta$$

を得る．$n(s,r)=1$ の場合は $s-r=w_r(s)\in\Delta$ となるから

$$r-s=-(s-r)\in\Delta.\quad \square$$

2. 基本系　　根系の基本系という概念が重要である．

定義 1.6　根系 Δ の部分集合 Π が次の2条件をみたしている時 Π を根系 Δ の**基本系**という．

(1)　Π の元は一次独立である．

(2)　Δ の各元は Π の元の整数係数の一次結合となりその係数はすべて $\geqq 0$ であるかまたはすべて $\leqq 0$ である．

Π を Δ の基本系とする時 Π の元の正係数一次結合となる根を**正根**という．正根全体のつくる Δ の部分集合を Π が定める**正系**といい Δ^+ と表わす．□

定理 1.7　根系は基本系をもつ．

この定理を証明するために E に全順序が与えられているとしよう．E に与えられた**全順序**とは E の元間の大小関係であって任意の2元 a, b が与えられれば $a>b, a=b, b>a$ のうちどれか一つだけが成り立ち，推移法則，$a>b, b>c \Rightarrow a>c$，および任意の正実数 λ と任意の $c\in E$ について

$$a>b \Longrightarrow \lambda a>\lambda b,\ a+c>b+c$$

が成り立つ関係である．E に全順序 $>$ が与えられた時

$$E^+=\{v\,|\,v>0\}$$

とおけば　(a)　E は $E^+, -E^+$，および $\{0\}$ の直和集合となり

(b)　$$u\in E^+, v\in E^+ \Longrightarrow u+v\in E^+, \lambda u\in E^+$$

が成り立つ．ここで λ は正実数である．逆に上の条件(a), (b)をみたす E の部分集合 E^+ が与えられた時，$a>b$ という関係を

$$a>b \Longleftrightarrow a-b\in E^+$$

により定義すれば関係 $>$ は E の全順序となる．

E に基 $\{e_i\}$ が与えられたとする．E の元 v を $v=\sum\alpha_i e_i$ と表わした時その

係数 $\alpha_1, \cdots, \alpha_n$ のうち零でない最初の数が正の時 $v \in E^+$ と定義する．このように定義された部分集合 E^+ は上の条件 (a), (b) をみたすことが容易に証明される．この E^+ が定める全順序を**基** $\{e_1, e_2, \cdots, e_n\}$ **により定義された全順序**という．（条件 (a), (b) を満足する部分集合は適当に選んだ基から上のようにして定まることが証明できる．）

さて E に全順序が与えられていると仮定し，任意の根系 $\varDelta$ に対して

$$P=\{r \in \varDelta \mid r>0\}$$

とおく．明らかに $\varDelta$ は P と $-P$ との和集合となる．P の元 r が

$$r=s+s', \qquad s \in P, \quad s' \in P$$

と書ける時 r は**分解可能**という．P の元で分解不可能な元全体のつくる集合を Π とおけば次の命題が成り立つ．

(1.8)　Π は $\varDelta$ の基本系である．Π が定める正系は P と一致する．

証明　(a)　まず P の各元が正整数を係数とする Π の元の一次結合として表わされることを証明しよう．そこでそのように表わすことのできない P の元の集合を I とおく．もし I が空集合でなければ（I は有限集合だから）与えられた順序で最小となる I の元を r とする．さて r は Π の元ではないから分解可能である．いま $r=s+s', s \in P, s' \in P$ とすれば $r>s$ および $r>s'$ が成り立つ．よって s も s' も I の元ではない．I の定義により r も I の元でなくなり矛盾がおこる．したがって I は空集合となり Π は基本系の条件 (2) をみたす．

(b)　$\Pi \ni r, s$ $(s \neq r)$ なら $(r, s) \leqq 0$ となることを証明しよう．もし $(r, s)>0$ ならば $n(r, s)>0$ であるから (1.5) により $t=r-s \in \varDelta$ を得る．もし $t \in P$ ならば $r=s+t$ となり r は分解可能である．これは r が Π の元であるという仮定に矛盾する．また $-t \in P$ なら $s=r+(-t)$ となり同様に矛盾がおこる．よって $(r, s) \leqq 0$ が成り立つ．

(c)　Π の元の間に一次関係式が成り立つと仮定すれば係数が同符号の項をまとめて

$$\sum a_r r=\sum b_s s \qquad (a_r>0, b_s>0)$$

と書くことができる．この左辺に現われる Π の元 r は右辺には現われない．そこで上式の左辺を v とおけば

$$0 \leqq (v, v)=(\sum a_r r, \sum b_s s)=\sum a_r b_s (r, s)$$

となる．一方，(b) により $(r,s)\leqq 0$ が成り立つから上式の右辺は $\leqq 0$. したがって $v=0$ を得る．ところで $r>0$ だからすべての r について $a_r=0$. 同様に $b_s=0$ となり矛盾がおこる．すなわち Π の元は一次独立である． □

定理 1.9 (a)　根系 $\varDelta$ の任意の元 r をとれば r を含む基本系がある．
(b)　r, s を一次独立な根とする．この時，次の性質 (1), (2) をもつ基本系 Π が存在する．(1)　$r\in\Pi$, (2)　Π の元 t があって s は r と t との負でない整数を係数とする一次結合となる．

証明　E の基 $\{e_i\}$ を $e_{l-1}=s, e_l=r$ となるように選ぶ．さて $\{e_i\}$ により定義される全順序を $>$ と表わし，この全順序が定める基本系を Π とおく．定義から明らかに r は最小の正根であるから r は分解不可能となる．よって定義により $r\in\Pi$ を得る．

上に定めた全順序により2番目に小さい正根を t とおく．明らかに t も分解不可能で Π の元である．ところで $s\geqq t$ だから全順序の定義により t は s と r との一次結合となる．それを $t=\alpha s+\beta r$ とおけば $t>0$ より α は正となる．よって $s=\alpha^{-1}(t-\beta r)$ となる．ところで任意の根を Π の元の一次結合として表わした時，係数の符号は一定である．$\alpha>0$ だから $\alpha^{-1}\beta\leqq 0$ となり (b) が証明される． □

注意　根系の条件 (ii) により $\varDelta$ の基本系 Π は E の基となる．そこで

$$\Pi=\{r_1, \cdots, r_l\}$$

とおいて前のように E に全順序を定義すればこの順序で正となる根の集合は Π が定める正系と一致している． □

3. Weyl 群との関係

まず次の命題を証明しよう．

(1.10)　Π を $\varDelta$ の基本系とする．この時，次の命題が成り立つ．

$$r\in\Pi, s\in\varDelta^+, s\neq r \Longrightarrow w_r(s)\in\varDelta^+.$$

証明　$\Pi=\{r_1, r_2, \cdots, r_l\}$ とおけば $s=\sum a_i r_i$ $(a_i\geqq 0)$ と書くことができる．$r\neq s$ だから $a_i>0, r_i\neq r$ をみたす i がある．よって

$$w_r(s)=s-n(s,r)r\in\varDelta$$

の右辺における r_i の係数は $a_i>0$ である．すなわち $w_r(s)$ の一つの係数が正だからすべての係数が $\geqq 0$ で $w_r(s)\in\varDelta^+$ となる． □

(1.11)　Π を $\varDelta$ の基本系とし Π の定める正系を $\varDelta^+$ とおく．

(a)　すべての $r\in\Pi$ について $(t,r)>0$ をみたす E の元 t がある.

(b)　E の元 t がすべての $r\in\Pi$ について $(t,r)>0$ をみたしていれば

$$\Delta^+=\{s\in\Delta\,|\,(t,s)>0\}$$

が成り立つ. Π は t により一意的に定まる.

証明　(a)　Δ^+ の元の和の半分を t とおく. さて $r\in\Pi$ ならば (1.10) により w_r は $\Delta^+-\{r\}$ を不変にするから

$$2t-r=w_r(2t-r)=2w_r(t)+r$$

すなわち $w_r(t)=t-r$ となる. また w_r は内積を変えないから

$$(t,r)=(w_r(t),w_r(r))=(t-r,-r)$$

を得る. よって $2(t,r)=(r,r)>0$ が成り立つ.

(b)　Δ^+ の元 s は Π の元の正係数一次結合であるから $(t,s)>0$ が成り立つ. 同様に $-\Delta^+$ の元 s' は $(t,s')<0$ をみたす. (1.8) により Π は Δ^+ の中で分解不可能な元の全体だから Π は Δ^+ により, したがって t により, 一意的に定まる. よって (b) が成り立つ. □

定理 1.12　根系を Δ, その Weyl 群を W とし Δ の基本系一つを Π とする.

(a)　E の任意の元を v とする. この時, 適当に $w\in W$ をとれば

$$(w(v),r)\geqq 0$$

がすべての $r\in\Pi$ について成り立つ.

(b)　Δ の基本系 Π' を任意にとれば $w(\Pi')=\Pi$ をみたす W の元 w がある.

(c)　Δ の任意の元 s について $w(s)\in\Pi$ をみたす W の元 w がある.

(d)　W は $\{w_r\ (r\in\Pi)\}$ により生成される.

証明　いま $W_1=\langle w_r\,|\,r\in\Pi\rangle$ とおき (a), (b), (c) を W_1 について証明しよう. Π の定める正系を Δ^+ とおく.

(a)　(1.11)の証明のように Δ^+ の元の和の半分を t とおき $(w(v),t)$ が最大となるように W_1 の元 w を選ぶ. そうすれば任意の $r\in\Pi$ について

$$(w(v),t)\geqq(w_rw(v),t)$$

となる. w_r は内積を変えないから $((w_r)^2=1$ より)

$$(w_rw(v),t)=(w(v),w_r(t))=(w(v),t-r)$$

を得る((1.11)の証明 (a) 参照). したがって任意の $r\in\Pi$ について

$$(w(v), r) \geqq 0$$

が成り立つ.

(b) (1.11)(a)により任意の $r' \in \Pi'$ について $(t', r') > 0$ をみたす E の元 t' がある. (a)により W_1 の元 w があって $w(t') = t$ とおけば $(t, r) \geqq 0$ がすべての $r \in \Pi$ について成り立つ. さて $(t, r) = (t', w^{-1}(r))$ となる. ここで t' はどの根とも直交しない ((1.11)(b)参照). $w^{-1}(r) \in \Delta$ であるから $(t, r) > 0$ となる. また (1.11)(b) により Π は t により一意的に定まる. よって $t = w(t')$ より $\Pi = w(\Pi')$ を得る.

(c) 定理 1.9 により s を含む基本系 Π' がある. さて $w(\Pi') = \Pi$ を満足する元 $w \in W_1$ があるから $w(s) \in \Pi$ を得る.

(d) 任意の $s \in \Delta$ について $w(s) = r \in \Pi$ をみたす W_1 の元 w が存在する. 一方, $ww_sw^{-1} = w_{w(s)} = w_r \in W_1$ となる. したがって

$$w_s = w^{-1}w_rw \in W_1$$

が成り立ち $W = W_1$ が証明される. □

根系 Δ の基本系の一つを Π とし Π が定める正系を Δ^+ とおく. 前定理により Δ の Weyl 群 W は $\{w_r\}$ $(r \in \Pi)$ により生成される. そこで任意の $w \in W$ について w を w_r $(r \in \Pi)$ の積として表わした時の最短表示の長さを $l(w)$ とおく. すなわち $w = w_{r(1)} \cdots w_{r(m)}$ $(r(i) \in \Pi)$ と表わすことのできる最小の m の値が $l(w)$ である. 特に $l(1) = 0$. また

$$n(w) = |w(\Delta^+) \cap (-\Delta^+)|$$

とおく. すなわち $n(w)$ は w により符号の変わる正根の数である. この時, 次の定理が成り立つ.

定理 1.13 $l(w) = n(w)$.

証明 いま $r \in \Pi$ とすれば (1.10) により w_r は r 以外の正根の符号を変えない. したがって

$$w(r) \in \Delta^+ \Longrightarrow n(ww_r) = n(w) + 1$$

$$w(r) \in -\Delta^+ \Longrightarrow n(ww_r) = n(w) - 1$$

となる. したがって w の最短表示を $w = w_{r(1)} \cdots w_{r(l)}$ とおけば

$$n(w) \leqq l = l(w)$$

が成り立つ. そこで $n(w) < l$ と仮定して矛盾を導こう. この時は

$$w_{r(1)}\cdots w_{r(j)}(r(j+1))\in -\varDelta^+$$

をみたす j $(j<l)$ がある．そこで $r=r(j+1)$ とおいて

$$w_{r(i)}\cdots w_{r(j)}(r)\in -\varDelta^+,\quad w_{r(i+1)}\cdots w_{r(j)}(r)\in \varDelta^+$$

を満足する i をとる．ところで $w_{r(i)}$ が符号を変える正根は $r(i)$ に限るから

$$w_{r(i+1)}\cdots w_{r(j)}(r)=r(i)$$

となる．この左辺を $w_0(r)$ と書けば $w_{r(i)}=w_0w_rw_0^{-1}$ が成り立つ．すなわち $w_{r(i)}w_0w_r=w_0$ となり上にあげた w の表示が最短であることに矛盾する．したがって $n(w)=l(w)$ が成り立つ． □

(1.14)　(a)　Π, Π' を基本系とすれば $w(\Pi')=\Pi$ をみたす $w\in W$ が一意的に定まる．

(b)　$w_0(\varDelta^+)=-\varDelta^+$ をみたす W の元 w_0 が唯一つ存在する．この元 w_0 の位数は2である．

証明　定理1.12(b)により $w(\Pi')=\Pi$ をみたす W の元 w がある．いま

$$w(\Pi')=w'(\Pi')=\Pi$$

と仮定すれば $x=w'w^{-1}$ は Π を不変にする．したがって $x(\varDelta^+)=\varDelta^+$ となり $n(x)=0$ が成り立つ．定理1.13により $l(x)=0$, すなわち $x=1$ を得る．よって $w(\Pi')=\Pi$ をみたす $w\in W$ は唯一つしかない．

Π を定める全順序を逆にすれば $-\varDelta^+$ がその順序に関する正根の全体となり対応する基本系は $-\Pi$ となる．よって $w_0(\Pi)=-\Pi$ をみたす W の元 w_0 が唯一つ存在する．w_0^2 は Π を不変にするから $w_0^2=1$ が成り立つ． □

注意　根系 $\varDelta$ が E の中に与えられた時 $\varDelta$ の元 r と直交する超平面を H_r とおく．E からこれらの超平面 H_r $(r\in\varDelta)$ を取り除いた残りの集合の連結成分は **Weyl 領域**とよばれている．一つ基本系 Π を定めれば

$$C=\{x\,|\,(x,r)>0\ \ \forall r\in\Pi\}$$

は一つの Weyl 領域となる((1.11)参照)．実際 C はすべての $s\in\varDelta^+$ について H_s が定める正半空間の共通部分である．さて定理1.12(a)により Weyl 群は Weyl 領域全体のつくる集合の上に可移に作用している．ところで $w\in W$ が C を不変にしていれば w は C の境界を不変にする．明らかに C は $r\in\Pi$ に対応する超平面 H_r によりかこまれているから $w(\Pi)=\Pi$ となり $w=1$ を得る(1.14)．すなわち任意の Weyl 領域 C' を C に移す Weyl 群の元は一つしかない．(1.11)(a)の証明で定義したように $\varDelta^+$ の元の和の半分を t とおけば $t\in C$ となる．任意に $v\in E$ をとり v を Weyl 群の元 w により動かした時 $w(v)$ と t とのつくる角が最小となるように w を選べば $w(v)$ はCの閉包

$\overline{C}$ に含まれている (定理 1.12 (a)). このように考えれば定理 1.12(a) の証明が直観的に把握されるであろう. □

4. Weyl 群の基本関係　Weyl 群の生成元の間に成り立つ基本関係を求めよう.

定理 1.15　根系 Δ の基本系を Π, Δ の Weyl 群を W とおく.

(a)　W の生成集合として $\{w_r\ (r\in\Pi)\}$ をとれば

$$(w_r w_s)^{m(r,s)}=1$$

が基本関係である. ここで r と s との間の角が $0°, 90°, 120°, 135°, 150°$ である時 $m(r,s)$ はそれぞれ $1, 2, 3, 4, 6$ となる.

(b)　W の生成集合として $\{w_s\ (s\in\Delta)\}$ をとれば

$$w_s{}^2=1, \quad w_r w_s (w_r)^{-1}=w_t \qquad (t=w_r(s))$$

が基本関係となる.

証明　(a)　W が Coxeter 群になることから容易に証明される (『群論』上 p. 354).

(b)　$W_1=\langle x_s \,|\, s\in\Delta, x_s{}^2=1, x_r x_s (x_r)^{-1}=x_t\ (t=w_r(s))\rangle$ とおき, W_1 と W とが同形であることを証明しよう. W では確かに

$$w_r w_s w_r{}^{-1}=w_t \qquad (t=w_r(s))$$

が成り立つから生成元とその間の関係によって定義された群の定義(『群論』上 p. 165) により W_1 から W の中への準同形 f があって $f(x_r)=w_r\ (r\in\Delta)$ が成り立つ. (a) により W は $w_r\ (r\in\Pi)$ により生成されその間の関係は

$$(w_r w_s)^{m(r,s)}=1$$

で与えられる. ところでこれらの関係はすべて $w_r{}^2=1$ および

$$w_r w_s w_r{}^{-1}=w_t \qquad (t=w_r(s))$$

から得られることが容易にわかる. したがって W_1 において

$$r, s\in\Pi \Longrightarrow (x_r x_s)^{m(r,s)}=1$$

が成り立つ. よって W から W_1 の中への準同形 g があって

$$g(w_r)=x_r \qquad (r\in\Pi)$$

が成り立つ. したがって fg は W の恒等写像となる. そこで gf が W_1 上の恒等写像であることを示せば証明が終了する. そのためには $r\in\Pi$ と制限しても x_r が W_1 を生成することを示せばよい. 任意の $s\in\Delta$ について $s=w(r)$ をみ

たす $r\in\Pi$ がある(定理 1.12). この時

$$w=w_{r(1)}\cdots w_{r(k)} \qquad (r(1),\cdots,r(k)\in\Pi)$$

となるから $x_{r(k)}x_rx_{r(k)}{}^{-1}=x_t$ $(t=w_{r(k)}(r))$ より始め，最後に

$$x_{r(1)}\cdots x_{r(k)}x_rx_{r(k)}{}^{-1}\cdots x_{r(1)}{}^{-1}=x_{w(r)}=x_s$$

を得る．すなわち各生成元が x_r $(r\in\Pi)$ の積となり W_1 は $\{x_r\}$ $(r\in\Pi)$ で生成される．したがって gf は W_1 の恒等写像となり g も f も同形である． ▯

5. 根の系列　任意の $r\in\Delta, s\in\Delta$ について $\{s+jr\in\Delta\}$ を s の r **系列**という．(ここで j は整数値をとる.)

定理 1.16　根系 Δ の 2 元 r,s をとり $s\neq\pm r$ と仮定する．

(a)　$\{j|s+jr\in\Delta\}$ は非負整数 p,q による区間 $[-p,q]$ に含まれる整数の集合と一致する．

(b)　$S=\{s+jr\in\Delta\}$ とおけば $w_r(S)=S$ が成り立つ．

(c)　$w_r(s-pr)=s+qr$, $p-q=n(s,r)$.

証明　$J=\{j|s+jr\in\Delta\}$ とおき J の最小数を $-p$，最大数を q とおく．明らかに p,q は非負整数である．J が区間 $[-p,q]$ に含まれる整数の集合と一致せず隙間 $[a+1,b-1]$ があると仮定して矛盾を導こう．さて

$$(s+ar,-r)\leqq 0, \quad (s+br,r)\leqq 0$$

が成り立つ(1.5)．しかし $a<b, (r,r)>0$ だから上の不等式は両立せず矛盾がおこる．したがって (a) が成り立つ．

いま $n=n(s,r)$ とおけば根系の条件 (iv) により n は整数で

$$w_r(s+jr)=s-(n+j)r \qquad (j\in J)$$

が成り立つ．よって $w_r(S)\subset S$ となる．S は有限集合だから $w_r(S)=S$ を得る．さらに上式より j が $-p$ から q まで一つずつ増えて行けば $-(n+j)$ は $p-n$ から $-q-n$ まで一つずつ減って行く．$w_r(S)=S$ より $p-n=q$ を得て (c) が証明される． ▯

注意　s の r 系列は $s-pr,\cdots,r,\cdots,s+qr$ である．そこで

$$t=s+qr$$

とおけば $w_r(t)=s-pr$ だから $n(t,r)=p+q$ が成り立つ．特に

$$p+q\leqq 3$$

である．定理 1.16 は (1.4) を用いて確かめることもできる． ▯

6. 根の高さ　根系 $\varDelta$ に基本系 $\varPi$ を定めれば $\varDelta$ の各元は $\varPi$ の元の整数係数一次結合として表わすことができる．いま $\varPi=\{r_1, \cdots, r_l\}$ とし

$$r=\sum a_i r_i$$

とすれば $\{a_i\}$ は同符号の整数である．この時 r の**高さ**を

$$\mathrm{ht}(r)=\sum a_i$$

と定義する．根の高さは基本系 $\varPi$ を定めた上で決まるので別に基本系 $\varPi'$ をとれば r は別の高さをもっている．

(1.17)　基本系 $\varPi$ に対応する高さを $\mathrm{ht}(r)$ と表わす．この時 E に適当な全順序 $>$ を定義して $\varPi$ の各元は正，さらに

$$r\in\varDelta, s\in\varDelta, r>s \Longrightarrow \mathrm{ht}(r)\geqq\mathrm{ht}(s)$$

が成り立つようにできる．

証明　高さ $\mathrm{ht}(r)$ は r に関して線形だから ht を E の線形写像 φ に拡張できる．そこで E の基 $\{x_i\}$ を $\varphi(x_1)=1, \varphi(x_i)=0$ $(i>1)$ となるように選び，基 $\{x_i\}$ により定義される全順序を $>$ とする．任意の根 r を $\{x_i\}$ の一次結合として表わした時 x_1 の係数は $\mathrm{ht}(r)$ である．したがってこの順序が (1.17) の条件をみたしていることは明らかであろう．□

根の高さについて帰納法を用いるのが便利なこともある．次の定理の証明はその一例である．

定理 1.18　根系 $\varDelta$ の基本系を一つ定めそれを $\varPi$ とおく．$\varPi$ が定める正系を $\varDelta^+$ とすれば $\varDelta^+$ の任意の元 s に対して基本系の元の列 $r_1, r_2, \cdots, r_n$ が定まり，すべての $i\leqq n$ について始めの i 項の和 $r_1+r_2+\cdots+r_i$ は $\varDelta$ の元であり，さらに $r_1+\cdots+r_n=s$ が成り立つ．

証明　根 r は基本系の元の正係数一次結合となる．すなわち

$$s=\sum a_r r \qquad (r\in\varPi, a_r\in\boldsymbol{Z}, a_r\geqq 0).$$

さて $(s, s)>0$ だから $\sum a_r(r, s)>0$ を得る．したがって少なくとも一つの $\varPi$ の元 r について $a_r>0$ および $(r, s)>0$ が成り立つ．もし s が $\varPi$ の元ならば定理は明らかに成り立つ．いま $s\notin\varPi$ と仮定すれば (1.5) により $s-r\in\varDelta$ となる．この時

$$\mathrm{ht}(s-r)=\mathrm{ht}(s)-1$$

だから $s-r\in\varDelta^+$．$\mathrm{ht}(s)$ に関する帰納法により定理が証明される．□

§2 複素単純 Lie 代数

後節で Chevalley 群を定義するが，それは複素数体上の各単純 Lie 代数に応じて定められるものである．ここで複素数体上の単純 Lie 代数の理論とその分類について復習しておこう．この節で述べる事実の証明は Lie 代数の教科書，例えば松島 [3] (p. 67—96) にゆずることにする．

しばらくの間，係数体は複素数体に限るから特にことわらない．半単純 Lie 代数を L，その Cartan 部分代数を H とする．H の双対空間を H^* とおく．また L の中の乗法を括弧積 $[x, y]$ で表わすことにする．任意の $\alpha\in H^*$ をとり $L_\alpha=\{x\,|\,[h, x]=\alpha(h)x \ \ \forall h\in H\}$ とおく．いま H^* の元 $\alpha\neq 0$ が $L_\alpha\neq\{0\}$ をみたす時 α を L の (Hに関する) **根**という．根の全体がつくる集合を Δ とおく．

$$\Delta=\{\alpha\,|\,\alpha \text{ は } L \text{ の根}\}.$$

この時 L の Cartan 分解が成り立つ．すなわち，直和分解

$$L=H+\sum L_\alpha \qquad (\alpha\in\Delta)$$

が成り立ち，各 α について L_α は 1 次元である．さて $y\longmapsto[x, y]$ は L の線形写像であるからこれを $\mathrm{ad}\,x$ と表わす．Lie 代数 L の **Killing 形式**とは

$$\mathrm{Tr}(\mathrm{ad}\,x\cdot\mathrm{ad}\,y)$$

で定義される双線形形式である．この Killing 形式の H 上への制限を B とおく．この時 B は H 上で非退化となる．よって任意の $\lambda\in H^*$ は

$$B(b_\lambda, h)=\lambda(h)$$

をみたす H の元 b_λ を一意的に定める．この対応 $\lambda\to b_\lambda$ を用いて H^* に内積を

$$(\lambda, \mu)=B(b_\lambda, b_\mu)=\mu(b_\lambda)$$

と定義することができる．これも非退化である．定義により $\Delta\subset H^*$ であるが H^* の元で根の実係数一次結合となるもの全体のつくる集合を E とおく．

$$E=\sum \boldsymbol{R}\alpha \qquad (\alpha\in\Delta).$$

重要なことは，上に定義した H^* の内積は E の上で正の定符号となることである．すなわちこの内積により E は Euclid 空間となり，Δ は §1 で定義した根系となる．H の次元を l とおけば Δ は l 個の元からなる基本系 Π を含んでいる．$\Pi=\{\alpha_1, \cdots, \alpha_l\}$ とおく．ここで

$$a_{ij}=2(\alpha_i, \alpha_j)/(\alpha_j, \alpha_j)$$

と定義すれば (1.8) の証明 (b) により $a_{ij}\leqq 0$ $(i\neq j)$, しかし $a_{ii}=2$ となる. また根系の条件 (iv) が満足されているから a_{ij} は整数である. 行列

$$C=(a_{ij})$$

を $\varDelta$ の Cartan 行列という. いま L' を半単純 Lie 代数としその Cartan 部分代数を H' とする. H' から出発して上のように Cartan 行列 C' が得られたとする. この時 $C=C'$ であれば L と L' とは同形になる. 逆に任意の根系 $\varDelta$ が与えられたとすれば行列 C が定まる. そして半単純 Lie 代数 L が存在し L に対応する根系の Cartan 行列が丁度 C と一致する(松島 [3] 第9章§3). このように半単純 Lie 代数の分類は根系の分類という幾何の問題に帰着される.

半単純 Lie 代数 L は単純なものの直和に分解する. L が単純であるための条件はその Cartan 行列が既約であること, すなわち C の行および列をどの様に入れ替えても

$$\begin{pmatrix} C' & 0 \\ 0 & C'' \end{pmatrix}$$

という形にならないことである. 既約な Cartan 行列を表現するため次のようなグラフを用いる. 基本系 Π の各元に一つずつ白丸を対応させ, これらの l 個の白丸を次の規則により線分で結ぶ. いま α_i と α_j との間の角を θ_{ij} とし

$\theta_{ij}=150^\circ \Longrightarrow \alpha_i$ ○≡○ α_i(3重)

$\theta_{ij}=135^\circ, (\alpha_i, \alpha_i)>(\alpha_j, \alpha_j) \Longrightarrow \alpha_i$ ○⟹○ α_j(2重)

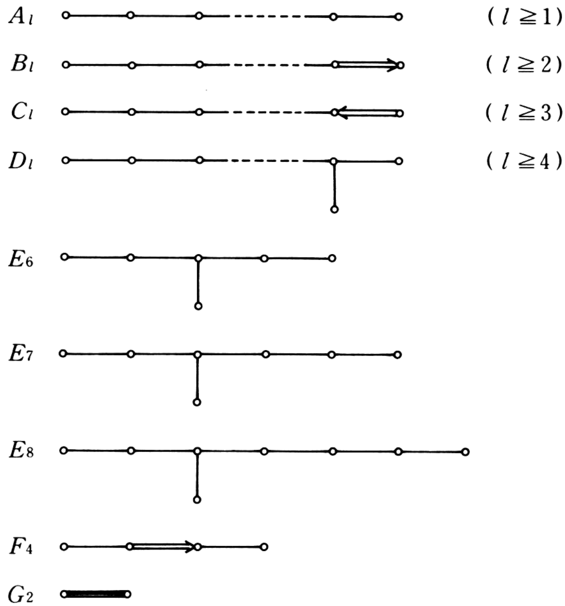
$\theta_{ij}=120^\circ \Longrightarrow \alpha_i$ ○—○ α_j

$\theta_{ij}=90^\circ \Longrightarrow \alpha_i$ ○　○ α_j(結ばない)

(1.3) および (1.8) の証明 (b) により θ_{ij} は上の4通り以外の値はとれない. この時, 既約な Cartan 行列に対応するグラフ(これを **Dynkin の図形**という)は次頁の表の通りである(松島 [3] 第10章).

以下 L は単純 Lie 代数とする. L の基を適当にとれば L の乗法定数がすべて整数となることを解説しよう. 根 α に対応して Cartan 部分代数の元 b_α が $B(b_\alpha, h)=\alpha(h)$ を満足するようにとれることは前に述べた. この時 b_α の実係数一次結合の全体を E' とおけば $\lambda\in E$ に $b_\lambda\in E'$ を対応させる写像は E から E' の上への等長写像となっている. したがって $\{b_\alpha\}$ は $\varDelta$ と同一視できる根系を

既約な Dynkin の図形



つくる．そこで b_α に直交する超平面に関する対称変換は w_α と同一視してよい．各 $\alpha \in \Delta$ について

$$h_\alpha = 2b_\alpha/(\alpha, \alpha) \qquad (\alpha \in \Delta)$$

とおけば次の重要な命題が成り立つ．

(2.1) 任意の根 β に対して $\beta(h_\alpha)$ は整数である．また

$$\Delta' = \{h_\alpha \mid \alpha \in \Delta\}$$

とおけば Δ' は根系で $\{h_r\ (r \in \Pi)\}$ が Δ' の基本系となる．

証明 実際 $\beta(h_\alpha)$ を計算してみれば

$$\beta(h_\alpha) = 2\beta(b_\alpha)/(\alpha, \alpha) = 2(\alpha, \beta)/(\alpha, \alpha)$$

となるから根系の条件 (iv) により $\beta(h_\alpha)$ は整数である．

つぎに Δ' が根系の条件を満足していることを証明しよう．h_α に直交する超平面に関する対称変換は $w = w_\alpha$ と一致するから $w(h_\beta) \in \Delta'$ を示そう．

$$w(h_\beta) = h_\beta - 2\{(h_\beta, b_\alpha)/(\alpha, \alpha)\} b_\alpha$$

$$=2(b_\beta-2\{(\beta,\alpha)/(\alpha,\alpha)\}b_\alpha)/(\beta,\beta).$$

ところで $b_\beta-2\{(\beta,\alpha)/(\alpha,\alpha)\}b_\alpha=b_{w(\beta)}$ が成り立つから

$$w(h_\beta)=h_{w(\beta)}\in\varDelta',$$

すなわち $\varDelta'$ は根系の条件 (iii) を満足している．また定義から

$$2(h_\alpha,h_\beta)/(h_\beta,h_\beta)=2(\beta,\alpha)/(\alpha,\alpha)$$

を得るので条件 (iv) も満足されている．他の条件が成り立つことは明らかだから $\varDelta'$ は根系となる．

いま $\varDelta$ の基本系 Π に対応する正系を $\varDelta^+$ とし $\varDelta''=\{h_\alpha|\alpha\in\varDelta^+\}$ とおけば明らかに $\varDelta''$ は $\varDelta'$ の正系である．そこで $\varDelta''$ に含まれる基本系を Π' とおけば $\varDelta''-\Pi'$ の元 h_α は $h_\alpha=h_\beta+h_\gamma$ $(\alpha\neq\beta,\alpha\neq\gamma,\beta\in\varDelta^+,\gamma\in\varDelta^+)$ と書ける．この式を書き直せば b_α が b_β と b_γ との正係数一次結合で表わせることになる．これは $\alpha\notin\Pi$ を示している．したがって $\Pi'\supset\{h_r|r\in\Pi\}$ を得る．ところで Π も Π' も共に l 個の元を含むから $\Pi'=\{h_r|r\in\Pi\}$ が成り立つ． ▯

注意　$\varDelta$ と $\varDelta'$ とは必ずしも同形ではない．$\varDelta$ の根がすべて同一の長さをもつ場合は $\varDelta'$ は $\varDelta$ を単に比例拡大（または縮小）したものだから $\varDelta'$ と $\varDelta$ は同形である．一般に (h_α,h_α) $(\alpha,\alpha)=4$ となる．よって

$$(\alpha,\alpha)\geqq(\beta,\beta)\Longleftrightarrow(h_\alpha,h_\alpha)\leqq(h_\beta,h_\beta)$$

が成り立つ．すなわち $\varDelta$ が B_l 型ならば $\varDelta'$ は C_l 型である． ▯

任意の根は基本系に属する根の整係数一次結合となるから $\{h_r\}$ $(r\in\Pi)$ は H の基となる．各 $\alpha\in\varDelta$ について L_α は1次元だからその生成元 e_α を次のように定める．まず $\alpha\in\varDelta^+$ の場合 e_α を定めた上で $e_{-\alpha}$ を

$$[e_\alpha,e_{-\alpha}]=h_\alpha\qquad(\alpha\in\varDelta)$$

を満足するように選ぶことができる（松島 [3] 第6章§2参照）．この時

$$\{h_\alpha\ (\alpha\in\Pi),e_\beta\ (\beta\in\varDelta)\}$$

は L の基となる．この基の元の間の括弧積は次の諸式を満足する．

$$[h_r,h_s]=0$$

$$[h_r,e_s]=n(s,r)e_s$$

(2.2)　$[e_r,e_{-r}]=h_r=h_\alpha$ $(\alpha\in\Pi)$ の整係数一次結合

$$[e_r,e_s]=0\qquad(r+s\notin\varDelta)$$

$$[e_r,e_s]=N_{r,s}e_{r+s}\qquad(r+s\in\varDelta).$$

ここで $n(s,r)=2(s,r)/(r,r)$ は整数である．第3式で h_r が基本系 Π に属する α に関する h_α の整係数一次結合となることは (2.1) から証明される．基 $\{e_r\}$ を適当に選んで最後の式における係数 $N_{r,s}$ も整数とすることができる．以下それについて解説しよう．乗法定数 $N_{r,s}$ の間には種々の関係式が成り立つ．いま根 r,s と共に $r+s$ も根であると仮定する．そして s の r 系列が $s-pr$ に始まり $s+qr$ で終るとすれば $q>0$ で

(2.3) $$N_{r,s}N_{-r,-s}(s,s)=-(p+1)q(r+s,r+s)$$

が成り立つ (松島[3] 補題7.13)．ところで $r+s$ が根となる場合は(1.4)により6通りに分類されるから各場合について $(s,s)(p+1)=q(r+s,r+s)$ が成り立つことが確かめられる．したがって

(2.4) $$N_{r,s}N_{-r,-s}=-(p+1)^2$$

となる．一方，Δ の基本系 $\{\alpha_1,\cdots,\alpha_l\}$ を $\{-\alpha_1,\cdots,-\alpha_l\}$ に変えても対応する Cartan 行列は変わらない．したがって同形定理により上の対応は L の自己同形により実現される．すなわち，L の自己同形 θ が存在して

$$\theta^2=1,\quad \theta(e_r)\in L_{-r}\qquad (r\in\Delta)$$

となる．そこで $\theta(e_r)=\lambda e_{-r}$ とおけば $\theta(e_{-r})=\lambda^{-1}e_r$ が成り立つ．いま $\mu^2\lambda=-1$ をみたす元 μ をとり e_r を μe_r に，e_{-r} を $\mu^{-1}e_{-r}$ に変えれば $\theta(\mu e_r)=\mu\lambda e_{-r}=-\mu^{-1}e_{-r}$ となる．すなわち，適当に e_r をとれば

(2.5) $$\theta(e_r)=-e_{-r}\qquad (r\in\Delta)$$

が成り立つようにできる．このように e_r をとりかえても $N_{r,s}$ 以外の乗法定数は変わらない．ところで，$[e_r,e_s]=N_{r,s}e_{r+s}$ の両辺の θ による像をとれば $[-e_{-r},-e_{-s}]=-N_{r,s}e_{-(r+s)}$ を得る．よって

$$N_{-r,-s}=-N_{r,s}\qquad (r,s\in\Delta)$$

が成り立つ．この式と (2.4) から

(2.6) $$N_{r,s}=\pm(p+1)$$

を得る．このように $\{e_r\}$ を適当に選べばすべての乗法定数を整数にすることができる．条件 (2.2) および (2.6) を満足する L の基を Chevalley の**標準基**という．条件 (2.2) をみたす L の基が (2.5) を満足するようにとれていればその基は Chevalley の標準基である．なお (2.6) における正負の符号については Tits [5] を参照されたい．

§3　単純 Lie 代数の例

1.　A_l 型　いま $(l+1, l+1)$ 型行列のうち対角和が 0 となるものの全体を L とおく．この時，括弧積 $[A, B]=AB-BA$（右辺は行列の積の差）に関して L は Lie 代数となる．さらに L は単純であることが証明される．

(i, j) 成分だけが 1 でその他の成分が 0 の行列を e_{ij} と表わせば

$$[[\sum a_{ij}e_{ij}, e_{kl}],\ e_{kl}]=-2a_{lk}e_{kl} \qquad (k\neq l)$$

$$[\sum a_i e_{ii}, e_{kl}]=(a_k-a_l)e_{kl} \qquad (k\neq l)$$

が成り立つから L のイデアル $I\neq\{0\}$ は少なくとも一つの組 (k, l) について e_{kl} を含む．そこで $[e_{ik}, e_{kl}]=e_{il}$ などの式から I はすべての e_{ij}, $e_{ii}-e_{jj}$ $(i\neq j)$ を含み $I=L$ となる．すなわち L は単純である．

いま L に含まれている対角行列全体のつくる集合を H とおけば H は L の Cartan 部分代数の一つである．H の元 $h=\sum\lambda_i e_{ii}$ について $\mathrm{ad}\,h$ を計算しよう．さて

$$(\mathrm{ad}\,h)e_{ij}=he_{ij}-e_{ij}h=(\lambda_i-\lambda_j)e_{ij} \tag{3.1}$$

が成り立つ．これは $h\longmapsto\lambda_i-\lambda_j$ が一つの根であることを示している．また $\{e_{ij}\}$ $(i\neq j)$ に対角行列を追加して L の基が得られる．$\mathrm{ad}\,h$ はこの基について対角行列となっている．そこで h および $h'=\sum\mu_i e_{ii}$ について

$$B(h, h')=\sum(\lambda_i-\lambda_j)(\mu_i-\mu_j),$$

ここで和は $i\neq j$ をみたすすべての組の上にわたる．しかし $i=j$ の項を含めても和は変わらない．$\sum\lambda_i=\sum\mu_i=0$ だから上式より

$$B(h, h')=2(l+1)\sum\lambda_i\mu_i$$

を得る．これが Killing 形式の H 上への制限 B である．H の双対空間 H^* を取扱うにあたり次の様に表わすことにする．まず

$$V=\{x=(x_0, x_1, \cdots, x_l)\,|\,x_i\in C\}$$

とおく．その双対空間 V^* の元 e_i を $e_i(x)=x_i$ $(i=0, 1, \cdots, l)$ と定義する．この時 $\{e_i\}$ は V^* の基となる．H の元 h に，その対角成分から成るベクトル $(\lambda_0, \lambda_1, \cdots, \lambda_l)$ を対応させれば H から V の中への線形写像が得られる．こうして H を V の中で方程式 $\sum x_i=0$ が定める超平面と同一視する．この時 V^* の元を H に制限することにより H^* の元が得られる．この写像 $V^*\to H^*$ は全射で，その核は $e=e_0+e_1+\cdots+e_l$ が生成する 1 次元空間である．さて

$$U=\{\sum a_i e_i \mid \sum a_i=0\}$$

とおけば $U\cap Ce=\{0\}$ だから(次元を考えれば) $U\cong H^*$ となる．そこで H^* を U と同一視する．$H\subset V$ だから

$$a=\sum a_i e_i \in U \Longrightarrow a(h)=\sum a_i\lambda_i.$$

§2の一般論に従って H の元 b_a を定義すれば

$$b_a=(1/2(l+1))\sum a_i e_{ii}.$$

よって U の中の内積 (a, a') は $(a'=\sum a'_i e_i$ とする時)

$$(a, a')=a'(b_a)=(1/2(l+1))\sum a_i a'_i$$

で与えられる．前に注意したように $h\longmapsto \lambda_i-\lambda_j$ が根である．そこで

$$\Delta=\{e_i-e_j\} \qquad (i\neq j)$$

は根系となり，$\Delta^+=\{e_i-e_j\ (i<j)\}$ は正系，

$$\Pi=\{p_1, p_2, \cdots, p_l\} \qquad (p_i=e_{i-1}-e_i)$$

が Δ^+ に含まれる基本系となる($i-j>1$ なら分解可能)．ここで

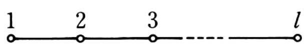
$$r=e_i-e_j \Longrightarrow -r=e_j-e_i$$

$$(r, r)=1/(l+1)$$

$$n(p_i, p_{i+1})=-1 \qquad (i=1, \cdots, l-1)$$

$$n(p_i, p_j)=0 \qquad (j\neq i-1, i, i+1)$$

が成り立つ．したがって Δ に対応する Dynkin の図形は A_l 型である．



根 $r=e_i-e_j$ に対応する H の元 b_r を計算すればその i 成分が $1/2(l+1)$，j 成分が $-1/2(l+1)$ でその他の成分は0となる．そこで一般論に従って h_r を定義すれば h_r の i 成分は 1，j 成分は -1 でその他の成分は0である．さて $e_r=e_{ij}$ と定めれば $e_{-r}=e_{ji}$ となるから

$$[e_r, e_{-r}]=e_{ii}-e_{jj}=h_r$$

が成り立つ．L の任意の行列 A を $-{}^tA$ に対応させる写像 θ は L の自己同形である．すなわち $\theta([A, B])=[\theta(A), \theta(B)]$ が成り立つ．ところで定義から明らかに $\theta(e_r)=-e_{-r}$ を得る．すなわち (2.5) が成り立つから

$$\{h_r\ (r\in\Pi), e_{ij}\}$$

は L の Chevalley 標準基である．Weyl 群 $W(\Delta)$ を $\{e_i\}$ 上の置換群とみれば $r=e_i-e_j$ に対応する元 w_r は e_i と e_j を入れかえている．よって w_r は互換に対応している．よって $W(\Delta)$ は $\{e_i\}$ 上の対称群 $\sum_{l+1}$ と同形である．

注意 $\Delta=\{e_i-e_j\}$ が根系の条件をみたしていることは容易に直接証明できる．H^* の内積は普通の内積の定数倍となっている．しかし角の計算にはこの定数は関係しないから $\{e_i\}$ が正規直交系をつくると仮定して角を計算してもよい．この注意は他の型の根系にもあてはまる． □

2. B_l 型 次の補題が必要になる．

補題 3.2 J を一つの (n,n) 型の行列とする．(n,n) 型行列のうち

$$L(J)=\{M|{}^tMJ+JM=0\}$$

と定義される集合 $L(J)$ は括弧積により Lie 代数となる．

証明 M, N が共に $L(J)$ に属していれば ${}^tMJ=-JM, {}^tNJ=-JN$ が成り立つ．よって

$$\begin{aligned}{}^t[M,N]J&=({}^tN{}^tM-{}^tM{}^tN)J\\&=JNM-JMN=-J[M,N]\end{aligned}$$

を得るから $[M,N]\in L(J)$ が成り立つ．$L(J)$ が線形空間であることは明らかだから $L(J)$ は括弧積により Lie 代数となる． □

さて $n=2l+1$ を奇数とし

$$J_B=J=\begin{pmatrix}2&0&0\\0&0&I\\0&I&0\end{pmatrix} \qquad (I \text{ は } (l,l) \text{ 型単位行列})$$

によって $L(J)$ を定義する．この $L(J)$ も単純 Lie 代数であることが A_l 型の場合と同様に証明される．以下 $L(J)$ が B_l 型であることを証明しよう．いま $A\in L(J)$ を適当に小行列に分け ${}^tAJ+JA=0$ となる条件を求めれば

$$\begin{pmatrix}a&a_1&a_2\\b_1&A_1&A_2\\b_2&A_3&A_4\end{pmatrix}\in L(J)\Longleftrightarrow \begin{matrix}a=0, & 2a_1=-{}^tb_2,\\ 2a_2=-{}^tb_1, & {}^tA_1=-A_4,\\ {}^tA_2=-A_2, & {}^tA_3=-A_3\end{matrix}$$

を得る．ここで a_1, a_2 は $(1,l)$ 型，A_i は (l,l) 型の行列である．

行列の行および列を $0,1,2,\cdots,2l$ によって番号づければ $L(J)$ の基として対角行列 $e_{ii}-e_{l+i,l+i}$ $(i=1,2,\cdots,l)$ に加えて次の行列をとることができる．

$$u_i = e_{0i} - 2e_{l+i,0}$$
$$v_i = 2e_{i0} - e_{0,l+i}$$
$$u_{ij} = e_{ij} - e_{l+j,l+i} \qquad (i \neq j)$$
$$s_{ij} = e_{i,l+j} - e_{j,l+i} \qquad (i < j)$$
$$t_{ij} = e_{l+j,i} - e_{l+i,j} \qquad (i < j)$$

(t_{ij} は s_{ij} の転置行列)．ここで i, j は1から l までの整数値をとる．この場合も対角行列の全体 H が $L(J)$ の Cartan 部分代数となる．そこで

$$h = \sum \lambda_i (e_{ii} - e_{l+i,l+i})$$

について ad h を計算すれば次の結果を得る．

$$[h, u_i] = -\lambda_i u_i$$
$$[h, v_i] = \lambda_i v_i$$
$$[h, u_{ij}] = (\lambda_i - \lambda_j) u_{ij} \qquad (i \neq j)$$
$$[h, s_{ij}] = (\lambda_i + \lambda_j) s_{ij} \qquad (i < j)$$
$$[h, t_{ij}] = -(\lambda_i + \lambda_j) t_{ij} \qquad (i < j).$$

すなわち $h \longmapsto \pm\lambda_i, \lambda_i - \lambda_j\ (i \neq j), \pm(\lambda_i + \lambda_j)\ (i < j)$ が根である．そこで Killing 形式を H 上で計算すれば

$$B(h, h') = \sum r(h) r(h'),$$

ここで和はすべての根 r にわたる．$h' = \sum \mu_i (e_{ii} - e_{l+i,l+i})$ とおけば

$$B(h, h') = (4l-2) \sum \lambda_i \mu_i$$

となる．いま H^* の元 e_i を $e_i(h) = \lambda_i$ と定義すれば $H^* \ni a = \sum a_i e_i$ に対応する H の元 b_a は

$$(4l-2) b_a = \sum a_i (e_{ii} - e_{l+i,l+i})$$

をみたす．したがって a と $a' = \sum b_i e_i$ との H^* の中での内積は

$$(a, a') = a'(b_a) = \sum a_i b_i / (4l-2)$$

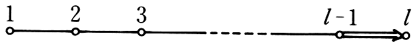
である．根の集合 Δ は $l \geqq 2$ ならば

$$\Delta = \{\pm e_i, e_i - e_j\ (i \neq j), \pm(e_i + e_j)\ (i < j)\}$$

で $\Delta^+ = \{e_i, e_i - e_j\ (i < j), e_i + e_j\ (i < j)\}$ が正系，

$$\Pi = \{e_1 - e_2, e_2 - e_3, \cdots, e_{l-1} - e_l, e_l\}$$

が基本系となる．対応する Dynkin の図形は



となり，この根系は B_l 型である．

各根 r に対応する元 h_r を表にまとめておく．(r の代りに L_r の生成元 e_r をとり $h_r=h(e_r)$ と書いた．)

$$h(u_i)=-2(e_{ii}-e_{l+i,l+i})$$
$$h(v_i)=2(e_{ii}-e_{l+i,l+i})$$
$$h(u_{ij})=e_{ii}-e_{l+i,l+i}-e_{jj}+e_{l+j,l+j} \qquad (i\neq j)$$
$$h(s_{ij})=e_{ii}-e_{l+i,l+i}+e_{jj}-e_{l+j,l+j} \qquad (i<j)$$
$$h(t_{ij})=-e_{ii}+e_{l+i,l+i}-e_{jj}+e_{l+j,l+j} \qquad (i<j).$$

括弧積を計算して $[e_r, e_{-r}]=h_r$ $(r\in\Delta)$ の成り立っていることを確かめることができる．この場合 $M\in L(J)$ でも $-{}^tM\in L(J)$ とは限らないが

$$T^{-1}=\begin{pmatrix}2 & 0 & 0\\ 0 & I & 0\\ 0 & 0 & I\end{pmatrix}$$

とおけば $TJT=J^{-1}$ だから $M\in L(J)\Rightarrow -T{}^tMT^{-1}\in L(J)$ となる．明らかに $\theta: M\longmapsto -T{}^tMT^{-1}$ は $L(J_B)$ の自己同形で

$$\theta(u_i)=-v_i,\quad \theta(u_{ij})=-u_{ji},\quad \theta(s_{ij})=-t_{ij}$$

が成り立つ．すなわち (2.5) が成り立つから基

$$\{h_r\ (r\in\Pi), u_i, v_i, u_{ij}, s_{ij}, t_{ij}\}$$

は $L(J_B)$ の Chevalley の標準基である．

B_l 型の根系の Weyl 群を W とおけば前と同様，根 $r=e_i-e_j$ に対応する W の元 w_r は e_i と e_j とを入れ替える．また根 e_i に対応する元は e_i と $-e_i$ とを入れ替える．したがって W の元 w に

$$w(e_i)=\varepsilon(i)e_{\sigma(i)} \qquad (\varepsilon(i)=\pm 1)$$

によって定められる置換 σ と符号変更 ε とが対応する．いま

$$w\longmapsto(\sigma,\varepsilon),\quad w'\longmapsto(\tau,\eta)$$

とすれば $ww'(e_i)=w(\eta(i)e_{\tau(i)})=\eta(i)\varepsilon(\tau(i))e_{\sigma\tau(i)}$ より

$$ww'\longmapsto(\sigma\tau, \varepsilon\tau\cdot\eta)$$

となる．ここで $\varepsilon\tau, \varepsilon\tau\cdot\eta$ はそれぞれ符号変更の上に定義される τ の作用と符号変更の積である．明らかに $w\longmapsto\sigma$ は W から対称群 Σ_l の上への準同形でその核は符号変更全体のつくる可換群 A である．A は位数 2^l の基本可換群，すなわち各元の位数が 2 または 1 である．実際，Σ_l を自然に l 文字の置換群とみてつくった Z_2 wr Σ_l が Weyl 群と同形になる(『群論』上 p. 267)．W の位数は $2^l(l!)$ である．

3. C 型　$n=2l$ は偶数とし $J=J_C$ として

$$J=\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \qquad (I \text{ は } (l,l) \text{ 型単位行列})$$

をとる．この時 $L(J)$ が C 型の単純 Lie 環となる．単純であることの証明は省略して $L(J)$ が C 型であることだけ示そう．$L(J)$ の元 A を (l,l) 型の小行列に分けて $A\in L(J)$ となるための条件を求めれば

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}\in L(J) \Longleftrightarrow \begin{array}{l} {}^tA_1=-A_4, \quad {}^tA_2=A_2 \\ {}^tA_3=A_3 \end{array}$$

を得る．行と列とを $1,2,\cdots,n$ を用いて番号をつければ A の基として対角行列および次の各行列がとれる．(i,j は 1 から l までの値をとる.)

$$u_{ij}=e_{ij}-e_{l+j,l+i} \qquad (i\neq j)$$
$$s_{ij}=e_{i,l+j}+e_{j,l+i} \qquad (i<j)$$
$$t_{ij}=e_{l+j,i}+e_{l+i,j} \qquad (i<j)$$
$$s_i=e_{i,l+i}$$
$$t_i=e_{l+i,i}.$$

$L(J)$ の対角行列全体を H とおけば H は $L(J)$ の Cartan 部分代数となる．

$$h=\sum\lambda_i(e_{ii}-e_{l+i,l+i})$$

について ad h を計算しよう．結果は次の通り．

$$[h, s_i]=2\lambda_i s_i$$
$$[h, t_i]=-2\lambda_i t_i$$
$$[h, u_{ij}]=(\lambda_i-\lambda_j)u_{ij}$$
$$[h, s_{ij}]=(\lambda_i+\lambda_j)s_{ij} \qquad (i<j)$$
$$[h, t_{ij}]=-(\lambda_i+\lambda_j)t_{ij} \qquad (i<j).$$

そこで Killing 形式を H の上で計算すれば $(h'=\sum\mu_i(e_{ii}-e_{l+i,l+i}))$

$$B(h, h')=4(l+1)\sum\lambda_i\mu_i$$

となる．前と同様 H^* の元 e_i を $e_i(h)=\lambda_i$ と定義すれば $a=\sum a_ie_i\in H^*$ に対応する H の元 b_a は

$$b_a=(1/4(l+1))\sum a_i(e_{ii}-e_{l+i,l+i})$$

である．したがって H^* の内積は a と $a'=\sum b_ie_i$ に対して

$$(a, a')=a'(b_a)=(1/4(l+1))\sum a_ib_i$$

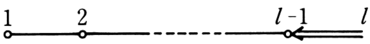
となる．根の集合 Δ は $l\geqq 2$ の時

$$\Delta=\{\pm 2e_i, e_i-e_j\ (i\neq j), \pm(e_i+e_j)\ (i<j)\}$$

で $\Delta^+=\{2e_i, e_i-e_j\ (i<j), e_i+e_j\ (i<j)\}$ は正系

$$\Pi=\{e_1-e_2, e_2-e_3, \cdots, e_{l-1}-e_l, 2e_l\}$$

が基本系となる．対応する Dynkin の図形は



でこの根系は C_l 型である．Weyl 群は B_l 型の Weyl 群と同形である．

各根 r に対応する $h_r=h(e_r)$ は次の通りである．

$$h(u_{ij})=e_{ii}-e_{jj}-e_{l+i,l+i}+e_{l+j,l+j} \qquad (i\neq j)$$

$$h(s_{ij})=e_{ii}+e_{jj}-e_{l+i,l+i}-e_{l+j,l+j} \qquad (i<j)$$

$$h(t_{ij})=-e_{ii}-e_{jj}+e_{l+i,l+i}+e_{l+j,l+j} \qquad (i<j)$$

$$h(s_i)=e_{ii}-e_{l+i,l+i}=-h(t_i).$$

括弧積 $[e_r, e_{-r}]$ を計算すればそれが h_r に等しいことを確かめることができる．写像 $\theta: M\to -{}^tM$ は $L(J)$ の自己同形となる．各根について

$$\theta(e_r)=-e_{-r}$$

が成り立つから $\{h_r\ (r\in\Pi), u_{ij}, s_{ij}, t_{ij}, s_i, t_i\}$ は Chevalley の標準基である．

4. D 型　　$n=2l$ を偶数とし $J=J_D$ を

$$\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}$$

(ここで I は (l, l) 型単位行列) とおいて $L(J)$ を考える．行と列を $1, \cdots, n$ と番号をつければ B_l 型の場合の最初の行と列とを省いたものと全く同様である．そこで $L(J)$ の基として対角行列のほか u_{ij}, s_{ij}, t_{ij} (B_l 型の場合の記号をその

まま用いる）をとる．この場合 Killing 形式は

$$B(h, h')=4(l-1)\sum\lambda_i\mu_i$$

となる．したがって $a=\sum a_ie_i$ に対応する H の元 b_a は

$$b_a=(1/4(l-1))\sum a_i(e_{ii}-e_{l+i,l+i})$$

で H^* の内積は $(a, a')=(1/4(l-1))\sum a_ib_i$ で与えられる．

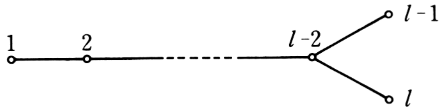
根の集合 $\varDelta$ は $l\geqq 2$ の時

$$\varDelta=\{e_i-e_j\ (i\neq j),\ \pm(e_i+e_j)\ (i<j)\}$$

で $\varDelta^+=\{e_j-e_i\ (i<j), e_i+e_j\ (i<j)\}$ が正系，その基本系は

$$\Pi=\{e_1-e_2, \cdots, e_{l-1}-e_l, e_{l-1}+e_l\}$$

である．これは $l=2$ の時は D_2 型，$l=3$ の時は A_3 型と一致する．しかし $l\geqq 4$ ならば対応する Dynkin の図形は



となり D_l 型である．各根に対応する h_r は B_l 型の場合と一致する．よって

$$\{h_r\ (r\in\Pi), u_{ij}, s_{ij}, t_{ij}\}$$

が Chevalley の標準基である．

根 e_i-e_j に関する対称変換は e_i と e_j を入れ替えるが e_i+e_j に対応する Weyl 群の元は $e_i\to -e_j, e_j\to -e_i$ と変換している．したがって D_l 型の場合，符号変更は対になっておこり

$$\prod\varepsilon(i)=1$$

が成り立つ．すなわち D_l 型の Weyl 群は B_l 型と同様 $W/A\cong\Sigma_l$ となる基本可換群 A を含んでいるが符号変更は上式をみたすものだけが可能で A の位数は 2^{l-1} となる．

5. E_8 型の根系　ここで例外型の単純 Lie 代数を具体的に書き上げることは省略し，根系だけを具体的に与えることにする．

いま 8 次元の Euclid 空間の中に正規直交系 $\{e_i\}, i=1, \cdots, 8$ をとり

$$\varDelta=\{\pm e_i\pm e_j\ (i<j), (1/2)\sum\varepsilon_ie_i\}$$

ここで $\varepsilon_i=\pm 1$ かつ和の中に $\varepsilon_i=-1$ となる項が偶数個あるものとする．こ

の集合 Δ が根系の条件をみたしていることを証明しよう．

まず Δ の各元 r は $(r,r)=2$ をみたしていることに注意する．よって根系の条件 (iv) は (r,s) が任意の r,s について整数であることと同値である．条件 (iv) を証明するに当って r,s の係数がすべて半整数である場合だけ考えれば十分である．さて r と s における e_i の係数の符号が丁度 x か所異なっていれば $(r,s)=(1/4)(8-x-x)=2-(x/2)$ である．ところで，r,s における負係数の数は共に偶数だから x も偶数で (r,s) は整数となる．よって条件 (iv) が成り立つ．

Δ の中で整係数の根だけ取り出せば D_8 型の根系が得られる．そこで r が整係数であれば対応する対称変換 w_r は整係数の根を整係数の根にうつしている．いま ξ,η を ±1 のいずれかとし $r=\xi e_i+\eta e_j$ $(i<j)$ とおく．さて

$$s=(1/2)\sum\varepsilon_i e_i \Longrightarrow (s,r)=(1/2)(\varepsilon_i\xi+\varepsilon_j\eta)$$

が成り立つ．$(r,s)=0$ ならば $w_r(s)\in\Delta$ は明らかである．$(r,s)=1$ ならば $\varepsilon_i=\xi, \varepsilon_j=\eta$ となるから $w_r(s)$ は s における e_i, e_j の係数の符号を変えたものと一致する．よって $w_r(s)\in\Delta$ となる．$(r,s)=-1$ ならば，同様に $w_r(s)\in\Delta$ が証明される．つぎに $r=(1/2)\sum\eta_k e_k$ とする．この時 s が整係数ならば上と同様に $w_r(s)$ は Δ の元となる．そこで s の係数も半整数とする．$s\neq\pm r$ とすれば

$$(r,s)=1 \Longrightarrow r \text{ と } s \text{ とは丁度 2 か所符号が異なる} \Longrightarrow w_r(s)\in\Delta$$

$$(r,s)=-1 \Longrightarrow \text{丁度 6 か所符号が異なる} \Longrightarrow w_r(s)=r+s\in\Delta.$$

したがっていずれの場合にも $w_r(s)\in\Delta$ となり根系の条件 (iii) が成り立つ．

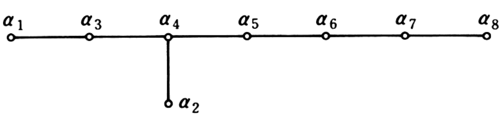
集合 Δ が条件 (i), (ii), (v) をみたしていることは自明だから Δ は根系である．この根系を E_8 と表わす．E_8 に含まれている根の数は

$$|\Delta|=4(8\cdot7)/2+2^7=240$$

である．部分集合 $\Delta^+=\{\pm e_i+e_j\ (i<j), (1/2)\sum\varepsilon_i e_i\ (\varepsilon_8=1)\}$ は正系で

$$\Pi=\{e_1+e_2, e_2-e_1, e_3-e_2, \cdots, e_7-e_6, \alpha_1\}$$

(ここで $\alpha_1=(1/2)(e_1-e_2-\cdots-e_7+e_8)$) が基本系となる．対応する図形は $\alpha_2=e_1+e_2, \alpha_{i+1}=e_i-e_{i-1}$ $(i=2,\cdots,7)$ とおいて



注意 7次元 Euclid 空間の中に $D_7=\{\pm e_i \pm e_j\}$ を与えた時それを含む8次元の根系は e_8-e_7 を基本系に加えた D_8 か，上の α_1 を加えた E_8 か，または α_1-e_1 を加えた根系に限ることが証明される．この最後の根系は e_1 に直交する超平面に関する対称変換で2番目の根系にうつされる．▯

6. E_7 型 E_8 型の根系のうち e_7+e_8 に直交するもの全体を Δ_1 とおく．もし $r\in\Delta_1$ ならば w_r は e_7+e_8 を不変にするから $w_r(\Delta_1)=\Delta_1$ が成り立つ．したがって Δ_1 は7次元の根系である．これを E_7 型という．対応する図形は上の E_8 図形から α_8 を除いたものである．根の数は次の通り．

$$|\Delta_1|=(4\cdot6\cdot5)/2+2+2^6=126.$$

7. E_6 型 Δ_1 の中で α_8 と直交する根の全体を Δ_2 とおく．$r\in\Delta_2$ ならば w_r は α_8 を不変にするから $w_r(\Delta_2)=\Delta_2$. したがって Δ_2 は6次元の根系となる．これを E_6 型という．対応する Dynkin の図形は E_8 の図形から α_8 と α_7 を除いたものである．この時，根の数は次式で与えられる．

$$|\Delta_2|=(4\cdot5\cdot4)/2+2^5=72.$$

8. F_4 型 4次元の Euclid 空間に正規直交系 $\{e_i\}$ をとり

$$\Delta=\{\pm e_i,\ \pm e_i\pm e_j\ (i<j),\ (1/2)\sum\varepsilon_i e_i\ (\varepsilon_i=\pm1)\}$$

とおく．Δ が根系の条件を満足していることは E_8 の場合と同様に（多少複雑になるが）証明される．いま

$$\Delta^+=\{e_i,\ e_i\pm e_j\ (i<j),\ (1/2)\sum\varepsilon_i e_i\ (\varepsilon_1=1)\}$$

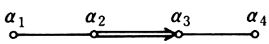
とおけば Δ^+ は正系でこれに含まれる基本系は

$$\Pi=\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$

ここで $\alpha_1=e_2-e_3, \alpha_2=e_3-e_4, \alpha_3=e_4$, および

$$\alpha_4=(1/2)(e_1-e_2-e_3-e_4)$$

である．対応する Dynkin の図形は



また，根の数は $|\Delta|=2\cdot4+(4\cdot4\cdot3)/2+2^4=48$ である．

9. G_2 型 G_2 型の根系は§1で既に述べた通りである．

注意 根系が与えられればそれに対応する Lie 代数が一意的に定まることが知られている（松島 [3] 定理9.5または Serre[8] Chap. VI, 定理9）．▯

§4 Chevalley 群の定義

1. 指数関数 まず線形写像 α の指数関数 $\exp\alpha$ を定義しよう．複素数を成分とする正方行列 A が与えられればその指数関数が

$$\exp A = I + A + A^2/2! + \cdots + A^n/n! + \cdots$$

により定義される．この右辺の第1項は A と同じ型の単位行列で左辺の各成分は絶対収束する無限級数で表わされている．もし T が可逆行列で A と同じ型ならば

$$\textbf{(4.1)} \qquad \exp(TAT^{-1}) = T(\exp A)T^{-1}$$

が成り立つ．これは $(TAT^{-1})^n = TA^nT^{-1}$ から明らかである．複素係数の空間 V に線形写像 α が与えられたとする．この時 $\alpha' = \exp\alpha$ は次の様に定義される．いま V に基 B を定め，α が B を用いて行列 A で表現されたとする．この時，基 B を用いて $\exp A$ により V の線形写像 α' が定まる．(4.1) により α' は V の基 B の取り方には無関係に一意的に定まるからそれを α の指数関数と定義して $\alpha' = \exp\alpha$ と表わす．指数関数は

$$\textbf{(4.2)} \qquad \alpha\beta = \beta\alpha \Longrightarrow \exp(\alpha+\beta) = (\exp\alpha)(\exp\beta)$$

を満足することを証明しよう．基を定めて α, β がそれぞれ行列 A, B により表現されたとする．この時 $AB = BA$ が成り立つから2項定理を用いて

$$\sum_{n=0}^{\infty} \frac{1}{n!}(A+B)^n = \sum_{n=0}^{\infty} \sum_{r=0}^{n} \frac{A^r B^{n-r}}{r!(n-r)!}$$

を得る．ここで右辺の和の順序を交換すれば各 r について，n に関して $n=r$ から ∞ まで和をとることになる．よって上式の右辺が $(\exp A)(\exp B)$ となり

$$\exp(A+B) = (\exp A)(\exp B)$$

を得る．すなわち (4.2) が成り立つ．

特に α と $-\alpha$ とは可換だから $\exp 0 = (\exp\alpha)(\exp(-\alpha))$ となる．ところで

$$\exp 0 = 1$$

だから $\exp\alpha$ は常に可逆で $(\exp\alpha)^{-1} = \exp(-\alpha)$ が成り立つ．

(4.3) 複素 Lie 代数 L の線形写像 δ が次の条件

$$\delta([x, y]) = [\delta x, y] + [x, \delta y]$$

をみたしている時 $\exp\delta$ は Lie 代数 L の自己同形である．

証明 まず n に関する帰納法により

$$\delta^n([x, y]) = \sum_{r=0}^{n} \binom{n}{r} [\delta^r x, \delta^{n-r} y]$$

の成り立つことが証明される．そこで $\theta = \exp \delta$ とおけば

$$\theta([x, y]) = \sum_{n=0}^{\infty} \sum_{r=0}^{n} \left[\frac{1}{r!} \delta^r x, \ \frac{1}{(n-r)!} \delta^{n-r} y \right]$$

を得る．この右辺で和の順序を変えれば前と同様に $[\theta x, \theta y]$ となる．よって θ は Lie 代数としての準同形である．一方，θ は可逆だから θ は L の自己同形となる．□

さて x を Lie 代数 L の任意の元とすれば ad x は (4.3) の仮定をみたしている．これは Lie 代数における Jacobi の法則を書き換えればよい．すなわち $[u, v] = -[v, u]$ を用いれば

$$[x[y, z]] + [y[z, x]] + [z[x, y]] = 0$$

より $\mathrm{ad}\, x\ ([y, z]) = [(\mathrm{ad}\, x)y, z] + [y, (\mathrm{ad}\, x)z]$ を得る．そこで (4.3) の系として複素 Lie 代数 L について次の結果が得られる．

系 $x \in L$ ならば $\exp(\mathrm{ad}\, x)$ は L の自己同形である．□

あとでこの自己同形の具体的な表示を求めることが重要になる．

定理 4.4 複素線形空間 V の線形写像からなる Lie 代数が与えられ L の中の積は $[x, y] = xy - yx$ である時，任意の $\alpha, \beta \in L$ について

$$(\exp\ \mathrm{ad}\, \alpha)\beta = (\exp \alpha)\beta(\exp \alpha)^{-1}$$

すなわち L の自己同形 $\exp(\mathrm{ad}\, \alpha)$ は $\exp \alpha$ による内部自己同形である．

証明 $\mathrm{ad}\, \alpha$ は L の線形写像で $(\mathrm{ad}\, \alpha)\beta = [\alpha, \beta] = \alpha\beta - \beta\alpha$ と定義されている．したがって帰納法により次式が証明される．

$$(\mathrm{ad}\, \alpha)^n \beta = \sum_{r=0}^{n} \binom{n}{r} \alpha^r \beta (-\alpha)^{n-r}.$$

前と同様，和の順序を変更することにより

$$(\exp\ \mathrm{ad}\, \alpha)\beta = \sum_{n=0}^{\infty} \sum_{r=0}^{n} \frac{\alpha^r}{r!} \beta \frac{(-\alpha)^{n-r}}{(n-r)!} = (\exp \alpha)\beta(\exp(-\alpha))$$

を得る．$\exp(-\alpha) = (\exp \alpha)^{-1}$ だから定理が成り立つ．□

2. 単純 Lie 代数の Z 形 §2 で述べたように任意の複素単純 Lie 代数 L に対応して根系 Δ が定まる．そして L は Chevalley の標準基

$$\{h_p\ (p\in\Pi),\ e_r\ (r\in\Delta)\}$$

をもっている．ここで Π は Δ の基本系の一つである．以下 Π および上にとった Chevalley の標準基を一つ定めておくことにする．この基の元の括弧積は (2.2) により定まっているから，そこで用いた記号をこの節でも用いることにしよう．一番大切なことは係数に現われる $n(r,s), N_{r,s}$ などがすべて整数となることである．そこで Chevalley の標準基の元の整係数一次結合の全体を

$$\mathscr{L}=\sum_{p\in\Pi}\boldsymbol{Z}h_p+\sum_{r\in\Delta}\boldsymbol{Z}e_r$$

とおけば $\mathscr{L}$ は整数環 $\boldsymbol{Z}$ 上の Lie 代数となっている．これを L の $\boldsymbol{Z}$ 形という．

Chevalley の標準基は根 r に対応する元 e_r と基本系 Π の元 p に対応する元 h_p とからなっている．しかし L の $\boldsymbol{Z}$ 形 $\mathscr{L}$ は標準基の $\{e_r\}$ の部分だけで定まり，基本系には無関係であることを証明しよう．

(4.5) $\{h_r\ (r\in\Delta)\}$ が生成する加法群を $\mathscr{H}$ とおけば L の $\boldsymbol{Z}$ 形は

$$\mathscr{L}=\mathscr{H}+\sum\boldsymbol{Z}e_r \qquad (\text{和は } r\in\Delta \text{ 全体にわたる})$$

となる．すなわち $\mathscr{L}$ は基本系 Π の選び方によらない．

証明 (2.1) により $\{h_r\ (r\in\Delta)\}$ は根系 Δ' をつくり，L の任意の基本系 Π について $\{h_p|p\in\Pi\}$ が Δ' の基本系となる．したがって任意の $h_r\ (r\in\Delta)$ は $\{h_p\}$ の整数係数一次結合となる．すなわち $h_r\in\sum\boldsymbol{Z}h_p$, よって $\mathscr{H}$ は L の $\boldsymbol{Z}$ 形 $\mathscr{L}$ に含まれている．逆に $\mathscr{L}$ が $\mathscr{H}+\sum\boldsymbol{Z}e_r$ に含まれることは明らかだから $\mathscr{L}=\mathscr{H}+\sum\boldsymbol{Z}e_r$ が成り立つ． □

さて L の $\boldsymbol{Z}$ 形は Lie 代数だから $\operatorname{ad} e_r$ は $\mathscr{L}$ を不変にする．実は

$$(\exp\operatorname{ad} e_r)\mathscr{L}\subset\mathscr{L}$$

が成り立つことを示そう．

(4.6) 任意の $r\in\Delta$ について $\operatorname{ad} e_r$ はベキ零である．任意の複素数 ζ について L の自己同形 $x_r(\zeta)$ を

$$x_r(\zeta)=\exp(\zeta\operatorname{ad} e_r)$$

とおく．この時，次式（$*$）が成り立つ．

$$(*)\qquad \begin{aligned} &x_r(\zeta)e_r=e_r\\ &x_r(\zeta)e_{-r}=e_{-r}+\zeta h_r-\zeta^2 e_r\\ &x_r(\zeta)h_s=h_s-n(r,s)\zeta e_r\\ &x_r(\zeta)e_s=e_s+\sum_{i=1}^{q}M_{r,s,i}\zeta^i e_{ir+s} \qquad (s\neq\pm r).\end{aligned}$$

この最後の式では $s \neq \pm r$, q は $qr+s \in \Delta$ を満足する最大の整数である．さらに $M_{r,s,i}$ は整数で次式で与えられる．

$$M_{r,s,i}=(1/i!)N_{r,s}N_{r,r+s}\cdots N_{r,(i-1)r+s}.$$

証明　(2.2) を用いて ad e_r を計算すれば

$$(\mathrm{ad}\, e_r)e_r=0$$
$$(\mathrm{ad}\, e_r)e_{-r}=h_r$$
$$(\mathrm{ad}\, e_r)h_r=-2e_r \qquad (n(r,r)=2)$$
$$(\mathrm{ad}\, e_r)e_s=N_{r,s}e_{r+s}$$

を得る．最後の式では $s \neq \pm r$ で，$r+s \notin \Delta$ ならば $N_{r,s}=0$ とおく．そこで s の r 系列を $-pr+s, \cdots, s, \cdots, qr+s$ とおけば

$$(\mathrm{ad}\, e_r)^2h_r=0, \quad (\mathrm{ad}\, e_r)^3e_{-r}=0, \quad (\mathrm{ad}\, e_r)^{q+1}e_s=0$$

となる．$q \leqq 3$ だから $(\mathrm{ad}\, e_r)^4=0$ となり前半が証明される．

定義により $x_r(\xi)$ は $\xi\,\mathrm{ad}\, e_r$ の指数関数だから（$*$）の諸式が成り立つ．残っている点は係数 $M_{r,s,i}$ が整数となることの証明である．さて s の r 系列を上のように定めれば (2.6) により $N_{r,s}=\pm(p+1)$ となる．$s+r$ の r 系列も上と同一であるが，対応する p の値は一つ増しているから

$$N_{r,r+s}=\pm(p+2),$$

同様に $N_{r,2r+s}=\pm(p+3), \cdots$ となり $M_{r,s,i}$ は整数となる．□

3. Chevalley 群の定義　変数 X をとり整数係数の多項式環を $\boldsymbol{Z}[X]$ とする．単純 Lie 代数 L の $\boldsymbol{Z}$ 形を $\mathcal{L}$ とおく．ここで係数環を $\boldsymbol{Z}$ から $\boldsymbol{Z}[X]$ に拡大すれば $\boldsymbol{Z}[X]$ 上の Lie 代数 $\boldsymbol{Z}[X]\otimes_{\boldsymbol{Z}}\mathcal{L}$ が得られる．(テンソル積の中で $1\otimes e_r$ などを略式に e_r と書くことにすれば) $B=\{h_r, e_s\}$ はその基となっている．そこで $\boldsymbol{Z}[X]$ 線形写像 $x_r(X)$ を基 B の各元に対し (4.6) の式($*$) に従い，ただし ξ は X に変えて定義する．

(4.7)　$x_r(X)$ は Lie 代数 $\boldsymbol{Z}[X]\otimes_{\boldsymbol{Z}}\mathcal{L}$ の自己同形である．

証明　$\theta=x_r(X)$ とおき $\theta[u,v]=[\theta u, \theta v]$ が任意の u, v について成り立つことを示そう．u, v 共に基 B の元である場合を考えれば十分である．そこで u, v を一組定め

$$\theta[u,v]=\sum P_w(X)w \qquad (w \in B)$$

とおく．係数 $P_w(X)$ は X の多項式である．同様に

$$[\theta u, \theta v]=\sum Q_w(X)w$$

とおけば $Q_w(X)$ も X の多項式である．任意の複素数 ζ について $x_r(\zeta)$ は L の自己同形であるから（(4.3)系）L の中で

$$x_r(\zeta)[u, v]=[x_r(\zeta)u, x_r(\zeta)v]$$

が成り立つ．定義により θ の中に現われる変数 X に ζ を代入すれば $x_r(\zeta)$ となるから上式より $P_w(\zeta)=Q_w(\zeta)$ がすべての ζ について成り立つ．したがって多項式として $P_w(X)=Q_w(X)$ となる．すなわち θ は Lie 代数の準同形である．また任意の複素数 ζ について $x_r(\zeta)x_r(-\zeta)=1$ が成り立つ．このことから上の論法を繰り返せば $x_r(X)x_r(-X)=1$ が証明される．すなわち θ は可逆で自己同形となる． □

この証明と同様にして $\boldsymbol{Z}[X, Y]\otimes\mathcal{L}$ の自己同形として次の命題が成り立つ．

(4.8) X, Y が可換な変数ならば $x_r(X+Y)=x_r(X)x_r(Y)$ が成り立つ． □

上の証明では $P_w(X)$, $Q_w(X)$ が X の多項式であることだけ用いたがこれらの多項式の係数はすべて整数である．さて任意の体 F をとり

$$L_F=F\otimes_{\boldsymbol{Z}}\mathcal{L}$$

とおく．L_F は係数体 F 上の Lie 代数で B がその基となっている．任意の元 $t\in F$ に対して L_F の線形写像 $x_r(t)$ を (4.6) の式（$*$）において ζ を t におき換えた式で定義する．

(4.9) 任意の $r\in\Delta, t\in F$ について $x_r(t)$ は Lie 代数 L_F の自己同形である．さらに $x_r(t+t')=x_r(t)x_r(t')$ が成り立つ．

証明 B は Chevalley の標準基だから $u, v\in B$ の時 $[u, v]$ は B の元の整係数一次結合となっている．よって $x_r(t)$ の定義から

$$x_r(t)[u, v]=\sum P_w(t)w$$

を得る．ここで $P_w(t)$ は(4.7)の証明において定義した整係数多項式 $P_w(X)$ において変数 X に t を代入したものである．前に述べたように $P_w(X)$ は整数係数の多項式であるから $P_w(t)$ が F の元として定まっている．同様に

$$[x_r(t)u, x_r(t)v]=\sum Q_w(t)w$$

となる．(4.7) の証明において示したように $P_w(X)=Q_w(X)$ だから $x_r(t)$ は L_F の自己準同形となる．(4.8) により

$$x_r(t+t')=x_r(t)x_r(t')$$

が成り立つ．よって $x_r(t)$ は可逆で L_F の自己同形となる． ▯

定義 4.10 複素数体上の単純 Lie 代数を L，対応する根系を Δ とする．任意の体を F とおけば，F 上の Δ **型の Chevalley 群**とは

$$\langle x_r(t) \mid r \in \Delta, t \in F \rangle$$

すなわち $\{x_r(t)\ (r \in \Delta, t \in F)\}$ が生成する $\mathrm{Aut}\, L_F$ の部分群と定義する．

注意 上に述べた解説では $\boldsymbol{Z}$ 形 $\mathcal{L}$ をつくる時 L の中に一つの特別な基 B をとり，それにより L_F を定義した．もともと根系 Δ も基 B も L の中に定めた Cartan 部分代数 H の取り方に依存している．しかし L は Δ により一意的に定まり，標準基 B をどの様にとっても L_F は L と F だけで(同形という意味で)一意的に定まり，Δ 型の Chevalley 群が Δ と F だけで一意的に定まる．しかしここではその証明を省略する(§9 節末の注意参照)． ▯

4. 一般 Chevalley 群 前節では Chevalley 群を Lie 代数 L_F の自己同形群として定義した．そのもととなるのは複素数体上の単純 Lie 代数の $\boldsymbol{Z}$ 形という概念である．$\boldsymbol{Z}$ 形 $\mathcal{L}$ は整数環上の Lie 代数であって $\mathrm{ad}\, e_r$ により不変である．しかしそれだけではなく，すべての n について $(\mathrm{ad}\, e_r)^n/n!$ により不変になる．このことは標準基の性質を用いて証明される．そしてこの点が Chevalley 群の構成を可能にする要点である．

一般に Lie 代数 L が作用している空間 V があればそれにより L の表現が定まる．この時その表現を用いて $GL(V)$ の部分群として一般 Chevalley 群が定義される．まずこの方法の概略を述べよう．(ここで用いる術語はあとで解説する．) さて複素数体上の半単純 Lie 代数を L とし，L が忠実に作用している表現加群を V，V が定める L の表現を φ とおく．この時 V の $\boldsymbol{Z}$ 形 $\mathcal{V}$ があってすべての n について

$$(\varphi(e_r)^n/n!)\mathcal{V} \subset \mathcal{V}$$

が成り立つことが証明される．また $\varphi(e_r)$ はベキ零になることも証明されるので任意の体 F と F の元 t について

$$x_r(t) = \exp t\varphi(e_r)$$

が $V_F = F \otimes_{\boldsymbol{Z}} \mathcal{V}$ の線形写像として定義される．これは可逆元で

$$\langle x_r(t) \mid r \in \Delta, t \in F \rangle$$

を体 F 上の (正確にいえば表現 φ による) Δ **型一般 Chevalley 群**という．

$V = L$ で φ が随伴表現の場合が前節で述べたもとの Chevalley 群である．

L が古典型の場合 L はある空間 V 上の行列のつくる Lie 代数である．よって L は自然に V に作用し，V により自然に L の表現 φ が定義される．この自然表現による A_l 型の Chevalley 群は $SL(l+1,F)$ と一致することをあとで証明する．

Δ 型の一般 Chevalley 群の中心による商群は Δ 型のもとの Chevalley 群であることが証明されるので一般 Chevalley 群はもとの Chevalley 群の中心拡大を与えている．だから群論的構造はほとんど同じであるが一般の群を考えることにより簡単になる問題が多い．

5. Lie 代数の表現　この節では Lie 代数も線形空間も係数体は複素数体と仮定する．さて L を Lie 代数，V を線形空間とする．L の V 上の**表現**とは L の元 x に V の線形写像 $\varphi(x)$ を対応させる関数 φ で

$$\text{(4.11)}\qquad \begin{aligned}&\varphi(\alpha x+\beta y)=\alpha\varphi(x)+\beta\varphi(y)\\&\varphi([x,y])=\varphi(x)\varphi(y)-\varphi(y)\varphi(x)\end{aligned}$$

がすべての $x,y\in L,\alpha,\beta\in \boldsymbol{C}$ について成り立つものである．この時 V を L の**表現空間**または L **加群**という．

L の元 x に L 上の線形写像 $\mathrm{ad}\,x$ を対応させれば L の表現が得られる．これを L の**随伴表現**という．($\mathrm{ad}\,x$ が条件 (4.11) をみたすことは $\mathrm{ad}\,x$ の定義と Jacobi の法則から容易に証明される．)

次に Lie 代数の包絡環という概念を定義しよう．それは多元環であるがこの本では**多元環**といえば乗法は結合法則をみたし，乗法に関する単位元が含まれているものと規約する．多元環 A が与えられた時 $[a,b]=ab-ba$ と定義すれば A はこの括弧積により Lie 代数となる．この Lie 代数を A_L と表わす．

定義 4.12　Lie 代数 L が与えられた時 L の**包絡環**とは次の条件をみたす組 (U,i) のことである．

(1)　U は多元環で i は L から U_L の中への準同形，

(2)　多元環 A と L から A_L の中への準同形 f があれば U から A の中への多元環準同形 θ で $\theta\circ i=f$ をみたすものが一意的に存在する．　□

上の定義により L の包絡環は普遍写像性質で定義されているから存在すれば（同形になるという意味で）一意的に定まる(『代数』II, p. 372 定理 1)．包絡環が存在することは次の様に証明される．L を線形空間と考えてその上のテ

ンソル代数を $T(L)$ とする(II §8参照). $T(L)$ の中で

$$[x, y]-x\otimes y+y\otimes x \qquad (x, y\in L)$$

という形の元が生成する $T(L)$ の両側イデアルを I とおき $U=T(L)/I$, さらに i を L から $T(L)$ の中への自然な埋め込みと商環 U への自然写像の合成とすれば組 (U, i) が L の包絡環になることが容易に証明される.

次の定理 (Poincaré-Birkhoff-Witt) が成り立つことが重要である.

定理 4.13 Lie 代数 L の包絡環を (U, i) とすれば i は単射である. L の基 $\{x_1, \cdots, x_n\}$ を定め U の元 $i(x_k)$ と x_k とを同一視すれば単項式

$$x_i^{a_i}x_j^{a_j}\cdots x_k^{a_k} \qquad (i<j<\cdots<k)$$

$(a_i, a_j, \cdots, a_k$ は正整数) は U の元となるがこれらの単項式全体が U の基をつくる(松島 [3] 定理9.3). □

今後 L の元 x と U の中の像 $i(x)$ とを同一視して L を U の部分集合と考える. そして写像 i は省略して単に包絡環 U と表わすことにする. 包絡環の定義より直ちに次の命題を得る.

(4.14) Lie 代数 L の包絡環を U とする. いま L 加群 V が与えられ L の V 上の表現を φ とおけば φ は U の表現に一意的に拡張される.

証明 V の線形写像の全体を E とおけば E は多元環となり表現 φ は L から Lie 代数 E_L の中への準同形となる(4.11). したがって包絡環の定義により U から E の中への多元環準同形 θ があって任意の $x\in L$ に対して

$$\theta(x)=\varphi(x)$$

が成り立つ(x と $i(x)$ を同一視している). $L\subset U$ だから θ は φ の拡張で

$$\theta(u_1u_2)=\theta(u_1)\theta(u_2) \qquad (u_i\in U)$$

などの式が成り立つ. そこで $u\cdot v=\theta(u)v$ $(v\in V)$ と定義することにより V が U 加群になり θ が U の V 上の表現となる. 多元環として U は L により生成されるから θ は φ の唯一の拡張である. □

あとで次の命題が必要になる.

(4.15) Lie 代数 L の表現加群 V と W が与えられた時 $V\otimes W$ に

$$x(v\otimes w)=xv\otimes w+v\otimes xw$$

と定義することにより $V\otimes W$ が L 加群となる.

証明 L の元 x に対応する $V\otimes W$ の線形写像が (4.11) をみたすことを確

かめればよい．たとえば (4.11) の第2式を証明してみよう．定義により

$$x(y(v\otimes w))=xyv\otimes w+yv\otimes xw+xv\otimes yw+v\otimes xyw$$

を得る．x と y とを入れ替えて $y(x(v\otimes w))$ を計算し上式から引けば

$$[x,y]v\otimes w+v\otimes[x,y]w$$

が残る．これが $[x,y](v\otimes w)$ に等しいから (4.11) の第2式が成り立つ．□

上に定義した作用により L 加群となった $V\otimes W$ を L 加群 V と W との**テンソル積**という．二つより多くの L 加群のテンソル積も同様に定義され

$$(V_1\otimes V_2)\otimes V_3\cong V_1\otimes(V_2\otimes V_3)\cong V_1\otimes V_2\otimes V_3$$

などが自然に同形となる．

6. 半単純 Lie 代数の包絡環　この節では L を半単純 Lie 代数とする．L に対応する根系の中に基本系 $\Pi=\{p_1,\cdots,p_l\}$ を選び，Π が定める正系を

$$\Delta^+=\{r_1,r_2,\cdots,r_N\}$$

と番号をつけることにする．そして Chevalley の標準基において p_i に対応する元を h_i, r_i に対応する元を e_i と表わすことにする．さて

$$A=(a_1,a_2,\cdots,a_N)$$

を整数 $a_i\geqq 0$ の組とする時 L の包絡環の元 e_A を

$$e_A=\prod e_i^{a_i}/(a_i!)$$

と定義する．ここで積は i について大きさの順にとる．上式で e_i の代りに負根 $-r_i$ に対応する標準基の元を入れた積を e_{-A} とおく．また $x\in L$ に対し

$$\binom{x}{k}=x(x-1)\cdots(x-k+1)/k! \qquad (k\text{ は正整数})$$

とおく．$k=0$ の場合，上の左辺は1を表わすと定義する．これも包絡環の元として確定する．整数 $b_i\geqq 0$ の組 $B=(b_1,\cdots,b_l)$ に対し

$$h_B=\prod_{i=1}^{l}\binom{h_i}{b_i}$$

とおく．定理 4.13 により $\{e_{-A}h_Be_C\}$ という形の元の全体が L の包絡環 U の基となる．(h_B の形が単にベキをとるのと少し違っているがこの形の基がとれることは明らかである.) そこで

$$\mathcal{U}=\sum \boldsymbol{Z}e_{-A}h_Be_C$$

とおけば $\mathcal{U}$ は包絡環 U の $\boldsymbol{Z}$ 形である．ここで次の重要な命題が成り立つ．

(4.16)　$\mathcal{U}$ は $e_r^n/(n!)$ が生成する $\boldsymbol{Z}$ 多元環と一致する．

証明 $e_r{}^n/(n!)$ $(r\in\Delta, n=1,2,\cdots)$ が生成する $\boldsymbol{Z}$ 上の多元環を $\mathcal{U}_0$ とおく．明らかに e_{-A}, e_C という形の元は $\mathcal{U}_0$ に含まれている．

まず $h_B\in\mathcal{U}_0$ を証明しよう．$X=e_r, Y=e_{-r}, H=h_r$ とおけば

$$[e_r, e_{-r}]=h_r \Longrightarrow XY=YX+H$$

同様に $XH=HX-2X$ および $HY=YH-2Y$ が包絡環の中で成り立つ．そこで m, n に関する帰納法により

$$\frac{X^m}{m!}\frac{Y^n}{n!}=\sum\frac{Y^{n-j}}{(n-j)!}\binom{H-m-n+2j}{j}\frac{X^{m-j}}{(m-j)!}$$

(ここで和は j について0から $\min(m,n)$ まで) の成り立つことが証明される．上式で $m=n$ とおけば右辺の和の最終項は

$$\binom{H}{n}$$

となる．一般に H の多項式が，H に任意の整数を代入した時，常に整数値をとるという条件をみたしていれば，その多項式は2項係数の形の多項式の整数係数一次結合となる．このことから n に関する帰納法により，2項係数の形の元はすべて $\mathcal{U}_0$ に含まれることが証明される．よって $h_B\in\mathcal{U}_0$ を得る．

e_r は (ad e_r として) L に作用しているから L は U 加群になる(4.14)．いま $e_r{}^n/(n!)$ の作用を X_n と表わせば (4.6) の証明からわかるように X_n は L の $\boldsymbol{Z}$ 形 $\mathcal{L}$ を不変にしている．(4.15) により $L\otimes L$ も U 加群になる．この時，作用の定義から

$$X_n(x\otimes y)=\sum X_k x\otimes X_{n-k}y$$

が成り立つので X_n は $\mathcal{L}\otimes\mathcal{L}$ を不変にしている．これは任意のテンソル積 $L\otimes L\otimes\cdots\otimes L$ についても同様に成り立つ．

次に $r\in\Delta^+$ と制限した時 $\{e_r{}^n/(n!)\}$ $(n=1,2,\cdots)$ が生成する U の部分 $\boldsymbol{Z}$ 多元環が $\sum\boldsymbol{Z}e_A$ と一致することを示そう．いま $\{e_i\}$ が生成する L の部分 Lie 代数を L_1 とおけば (2.2) により $\{e_i\}$ は L_1 の基となる．したがって定理4.13により $\{e_A\}$ が L_1 の包絡環 U_1 の基となる．そこで $\{e_i{}^n/(n!)\}$ が生成する部分環を U_2 とおけば U_2 の元は $\{e_A\}$ の複素数係数一次結合として表わすことができる．$A=(a_1, a_2, \cdots, a_N)$ の時，単項式 e_A の次数を $\sum a_i$ と定義する．さて U_2 の元 u を $\{e_A\}$ の一次結合として

$$(*) \qquad u=ce_A+\cdots, \quad A=(a_1, a_2, \cdots, a_N)$$

と表わした時，e_A が最高次数の単項式の一つとする．この時，係数 c が整数であることを証明すればよい．そこで u の $L\otimes\cdots\otimes L$ への作用を考える．ここで因子の数は e_A の次数 $\sum a_i$ に等しくする．各 i について e_{-r_i} を f_i とおき，a_i 個の f_i のテンソル積を並べて

$$f=(f_1\otimes\cdots\otimes f_1)\otimes\cdots\otimes(f_N\otimes\cdots\otimes f_N)$$

とおく．(f_1 は a_1 個，$\cdots$，f_N は a_N 個とるのである．) f は $\mathcal{L}\otimes\cdots\otimes\mathcal{L}$ の元である．上述の様に u は $\mathcal{L}\otimes\cdots\otimes\mathcal{L}$ を不変にするから

$$uf\in\mathcal{L}\otimes\cdots\otimes\mathcal{L}$$

となる．そこで uf の $\mathcal{H}\otimes\cdots\otimes\mathcal{H}$ 成分(H 成分と略称)を考える((4.5)参照)．単項式 e_B が u の展開式 $(*)$ に現われると仮定して e_Bf の H 成分を考える．e_B の次数が e_A の次数より小さければ(作用の定義から明らかなように) e_Bf の各成分を $\mathcal{H}$ の元とすることはできない．よって H 成分は 0 である．次数が同じでも $B\neq A$ ならば H 成分はやはり 0 となる($(\mathrm{ad}\, e_\alpha)e_\beta$ が $\mathcal{H}$ の元となるのは $\beta=-\alpha$ の時に限る)．そこで uf の H 成分は

$$ce_Af=c\prod(h_r\otimes\cdots\otimes h_r).$$

ここで右辺は各 $r=r_i$ について a_i 個の h_r をとったテンソル積である．定理 1.9(a) および (4.5) により h_r $(r\in\Delta)$ は $\mathcal{H}$ の直和因子を生成するから上式の右辺は零でない．$uf\in\mathcal{L}\otimes\cdots\otimes\mathcal{L}$ より係数 c は整数となる．すなわち $U_2=\sum \boldsymbol{Z}e_A$ が成り立つ．

$\mathcal{U}_0=\mathcal{U}$ を証明するために次の命題が必要となる．任意に 2 根 $r, s\in\Delta$ をとった時 $X=e_r, Y=e_s$ とおいて

$$(**) \qquad \frac{X^m}{m!}\frac{Y^n}{n!}=\frac{Y^n}{n!}\frac{X^m}{m!}+\cdots$$

となり省略した項は次数 $n+m$ 以下の単項式の整係数一次結合となることを証明しよう．$r+s=0$ の場合は証明の第 1 段階で述べた公式によりこの命題が成り立つ．また $r=s$ の場合は自明なことである．そこで r と s とは一次独立としてよい．この時は

$$e_re_s=e_se_r+[e_r, e_s]=e_se_r+N_{r,s}e_{r+s}$$

からはじめて帰納法により $(**)$ が成り立ち，省略した項は次数 $m+n$ 以下

の単項式の有理数係数一次結合となることが証明される．係数が整数となることを証明するために $\{ir+js\}$ という形の根 $(i\geqq 0, j\geqq 0)$ の全体を Δ_1 とおけば上に Δ^+ の場合に証明した結果が Δ_1 についてが成り立つ．そこで（＊＊）の右辺は $e_s, e_r, e_{r+s}, \cdots$ の順に整理された単項式の整係数一次結合となる．ところでこれらの単項式は一次独立だから，（＊＊）において省略した項は低次の単項式の整数係数一次結合となる．よって命題が成り立つ．

さて，$\mathcal{U}_0$ の元が与えられた時それを（＊＊）を用いて（与えられた順序に従って）整理することができる．その途中で $\mathcal{H}$ の元が現われるかも知れないが

$$(e_r{}^n/(n!))h_s=(h_s-nr(h_s))(e_r{}^n/(n!))$$

を用いて各単項式の中で h に関する項を一まとめにすることができる．この h に関する項は $\mathcal{H}$ の生成元 $h_1, \cdots, h_l$ の多項式である．現われ方から明らかなように h_i に任意の整数を代入すればその多項式は整数値をとる．したがってこれらの項は h_B という形の元の整係数一次結合となる．すなわち

$$\mathcal{U}_0=\sum \boldsymbol{Z} e_{-A}h_Be_C$$

となり(4.16)が成り立つ． □

7. 半単純 Lie 代数の表現論　次の Weyl の基本定理が成り立つ．

定理 4.17　半単純 Lie 代数の有限次元表現はすべて完全可約である．すなわち，表現加群は既約加群の直和に分解する．（松島［3］定理 4.8） □

L を半単純 Lie 代数としその Cartan 部分代数を H, L 加群を V, V の定める表現を φ とおく．H の双対空間 H^* の元 μ に対し

$$V_\mu=\{v\in V\mid \text{すべての } h\in H \text{ について } hv=\mu(h)v\}$$

と定義する．そして $V_\mu\neq\{0\}$ の時 μ を表現 φ の**重み**という．（随伴表現の重みは根にほかならない．）

(4.18)　任意の重み μ と根 r について $e_rV_\mu\subset V_{\mu+r}$ が成り立つ．

証明　任意の $h\in H$ に対し $he_r=e_rh+r(h)e_r$ が成り立つ．したがって v が V_μ の元ならば

$$he_rv=e_rhv+r(h)e_rv=(\mu(h)+r(h))e_rv$$

を得る．すなわち $e_rv\in V_{\mu+r}$ が成り立つ． □

よく知られているように $\mu, \nu, \cdots$ が互いに相異なる重みならば

$$V_\mu+V_\nu+\cdots$$

は直和になる．したがって有限次の表現 φ の相異なる重みは有限個しかない．そこで根の集合に全順序を定めた上で二つの重み μ, ν が $\mu-\nu\in\varDelta^+$ をみたす時 $\mu>\nu$ と定義する．この順序により極大となる重みを φ の**最高重み**という．

(4.19)　表現 φ の最高の重みを $\varLambda$ とおく．

(a)　任意の $r\in\varDelta^+$ について $e_rV_\varLambda=\{0\}$ が成り立つ．

(b)　任意の $r\in\varDelta$ について $\varLambda(h_r)$ は整数かつ $\geqq 0$ である．

証明　(4.18) により $e_rV_\varLambda\subset V_{\varLambda+r}$ となる．仮定により $\varLambda$ は最高の重みだから $\varLambda+r$ は重みではない．よって $V_{\varLambda+r}=\{0\}$ となり (a) が成り立つ．

記号を簡単にするために $x=e_r, y=e_{-r}, h=h_r, \varLambda(h)=\lambda$ とおく．(2.2) により $[x,y]=h, [h,y]=-2y$ が成り立つ．$V_\varLambda$ の元 v をとり

$$v_n=y^nv/(n!)\qquad (n=1,2,\cdots)$$

とおく．容易に $hv_n=(\lambda-2n)v_n$ を得る．そこで $v_0=v\neq 0$ と仮定すれば v_0, $v_1, \cdots$ のうち 0 でない元は $\varphi(h)$ の相異なる固有値に対応する固有ベクトルだから一次独立である．よって十分大きい m について $v_m=0$ となる．さて (a) により $xv=0$ を得る．よって帰納法により

$$xv_{n+1}=(\lambda-n)v_n$$

となることが証明される．いま $v_m\neq 0$ をみたす最大の整数を m とおく．上式を $m=n$ の場合に用いれば左辺が 0 となる．したがって右辺も 0 となるから $\lambda=m$ が成り立つ．すなわち，$\varLambda(h_r)$ は整数で $\geqq 0$ をみたす．　□

(4.20)　L を半単純 Lie 代数とし V を既約 L 加群とする．V による L の表現を φ, φ の最高の重みを $\varLambda$ とし v は $V_\varLambda$ の元で 0 でないと仮定する．

(a)　V は $e_{-A}v$ という形の元が生成する線形空間である．いま

$$A=(a_1,a_2,\cdots,a_N),\qquad \mu=\varLambda-\sum a_ir_i$$

とおけば $e_{-A}v\in V_\mu$ となる．(記号 e_{-A} は §4.6 参照.)

(b)　φ の重みは $\varLambda-\sum m_rr$ ($r\in\varPi, m_r$ は整数 $\geqq 0$) と書ける．

(c)　φ の最高の重みは $\varLambda$ だけに限る．$V_\varLambda$ は 1 次元である．

(d)　V は φ の重み全体にわたる直和 $V=\sum V_\mu$ に分解する．

証明　L の包絡環を U とする．明らかに Uv は V の L 部分空間であるが $\{0\}$ ではない．仮定により V は既約だから $V=Uv$ となる．定理 4.13 により単項式 $e_{-A}h_Be_C$ の全体が U の基となる．(4.19) (a) により $e_C\neq 1$ ならば

$e_C v=0$ となる．また h_B の定義から $h_B v=cv$ となり係数 c は

$$\prod\binom{\Lambda(h_i)}{b_i} \qquad (B=(b_1, \cdots, b_l))$$

に等しい．よって c は整数である(4.19)(b)．そこで Uv は $e_{-A}v$ という形の元により生成される空間である．e_{-A} の定義および (4.18) から (a) の成り立つことが証明される．

(a) により V は V_μ の元からなる (μ は重み全体を動く) 基をもつから (d) が成り立つ．任意の根 r は基本系に含まれる元の整係数一次結合として表わされるから (b) も成り立つ．

最後に (c) を証明しよう．Λ' が別の最高重みとする．(b) により

$$\Lambda'=\Lambda-\sum m_r r \qquad (m_r\geqq 0 \text{ は整数})$$

となる．一方，Λ' についてやはり (b) が成り立つから $\Lambda=\Lambda'-\sum n_r r$ となり $n_r\geqq 0$ は整数である．ところで Π の元は一次独立だから $m_r+n_r=0$ がすべての $r\in\Pi$ について成り立つ．m_r, n_r は共に $\geqq 0$ だから $m_r=n_r=0$．よって $\Lambda=\Lambda'$ を得る．(4.18) により $e_{-A}v\in V_\Lambda \Rightarrow e_{-A}=1$ を得るから V_Λ は1次元である． ▯

既約表現はその最高重みによって決定される．すなわち半単純 Lie 代数の二つの既約表現が同一の最高重みをもてば，それらの表現は同値である(松島[3]定理9.4)．また $\Lambda\in H^*$ が $\Lambda(h_r)$ はすべて非負整数であるという条件をみたしていれば，Λ を最高重みとする有限次元の既約表現が存在する(松島[3]定理9.6)．

さて目標は次の定理を証明することであった．

定理 4.21 半単純 Lie 代数 L をとり，V を L 加群とする．L の包絡環の $\boldsymbol{Z}$ 形を $\mathcal{U}$ とおく((4.16)の前の定義参照)．この時 V の $\boldsymbol{Z}$ 形 $\mathcal{V}$ があって

$$\mathcal{U}\mathcal{V}\subset\mathcal{V}$$

が成り立つ．(この条件をみたす V の $\boldsymbol{Z}$ 形を**許容 $\boldsymbol{Z}$ 形**という．) V が既約 L 加群の場合，その表現の最高重みを Λ とし $v\neq 0$ を V_Λ の元とする．この時 $\mathcal{U}v=\mathcal{V}$ は V の許容 $\boldsymbol{Z}$ 形である．

証明 定理4.17により V は既約 L 加群の直和に分解する．よって各直和因子の中に $\mathcal{U}$ 不変な $\boldsymbol{Z}$ 形が含まれていることを証明すればよい．そこで V は

既約と仮定する.

最高重みを Λ とおき $v\in V_\Lambda-\{0\}$ とする. (4.20) の証明のはじめに述べた様に $\mathcal{V}=\mathcal{U}v$ は $\{e_{-A}v\}$ の整数係数一次結合となる. (4.20) によりこれらの元が生成する空間は V と一致する. また V に現われる重みは有限個しかないので $e_{-A}v$ のうち 0 でない元は有限個しかない. よって $\mathcal{V}$ は有限生成の加法群である. (4.16) により $\mathcal{U}$ は多元環だから $\mathcal{V}$ は $\mathcal{U}$ 不変である. よって定理を証明するには, $\mathcal{V}$ の中で $\boldsymbol{Z}$ 上一次独立な元の集合 $\{v_i\}$ は $\boldsymbol{C}$ 上でも一次独立であることを証明すればよい. $\{v_i\}$ に含まれる元数に関する帰納法による.

まず任意の $u\in\mathcal{U}$ について uv の V_Λ 成分は v の整数倍であることを証明しよう. u は $e_{-A}h_B e_C$ という形の元の整数係数一次結合として表わすことができる. uv の V_Λ 成分は $e_C=e_{-A}=1$ をみたす項以外からは出て来ない. 前にも注意したように h_Bv は v の整数倍となるから uv の V_Λ 成分は v の整数倍である. そこで $\mathcal{V}$ の任意の元 x に対し, その V_Λ 成分を $\lambda(x)v$ と表わすことにする(V_Λ は V の直和因子である (4.20) (d)).

さて $\{v_i\}$ は $\boldsymbol{Z}$ 上一次独立と仮定し $\sum c_iv_i=0$ とおく. $u\in\mathcal{U}$ に対し

$$\sum c_in_i=0 \qquad (n_i=\lambda(uv_i)\in\boldsymbol{Z})$$

が成り立つ. $v_1\neq0$ かつ V が既約だから $V=Uv_1$ となる. $\mathcal{U}$ は U の $\boldsymbol{Z}$ 形だから $\lambda(\mathcal{U}v_1)\neq0$, すなわち $\mathcal{U}$ の元 u を適当に選べば $n_1\neq0$ となる. そこで $w_i=n_1v_i-n_iv_1$ $(i=2,3,\cdots)$ とおけば $\{w_i\}$ は $\boldsymbol{Z}$ 上一次独立である. よって帰納法の仮定により $\{w_i\}$ は $\boldsymbol{C}$ 上でも一次独立である. ところで n_i の定義により $\sum c_iw_i=0$ となるから $c_2=\cdots=0$ を得る. $v_1\neq0$ だから c_1 も 0 となり $\{v_i\}$ は $\boldsymbol{C}$ 上一次独立となる. よって $\mathcal{V}$ は V の $\boldsymbol{Z}$ 形である. □

8. 一般 Chevalley 群の定義 L を半単純 Lie 代数とし L 加群 V をとる. V による L の表現を φ とすれば L の元 $x\neq0$ が V に自明に作用していることもあり得る. しかし $I=\{x\in L\,|\,\varphi(x)=0\}$ とおけば I は L のイデアルとなる. そこで $L_0=L/I$ とおけば V は自然に L_0 加群となる. そして L_0 では 0 だけが V に自明に作用している. すなわち L_0 の表現は**忠実**である. また L_0 も半単純だから, はじめから L の表現 φ は**忠実**と仮定する.

L の Chevalley の標準基 $\{h_i,e_r\}$ を定める. 各 $r\in\Delta$ について $\varphi(e_r)$ は V の線形写像だから

$$x_r(\zeta)=\exp \zeta\varphi(e_r)$$

が任意の複素数ζについて定義される．§4.1 で述べたようにこれは V の可逆な線形写像となる．そこで

$$\langle x_r(\zeta) \mid r\in\Delta, \zeta\in \boldsymbol{C}\rangle$$

が $\boldsymbol{C}$ 上の**一般 Chevalley 群**である．次の命題が成り立つ．

(4.22) 各 $r\in\Delta$ について $\varphi(e_r)$ はベキ零である．

証明 定理 4.17 により (4.20) (d) が一般の（既約とは限らない）L 加群について成り立つ．すなわち $V=\sum V_\mu$ と直和分解する．(4.18) により

$$\varphi(e_r)^n V_\mu\subset V_{\mu+nr}$$

が成り立つ．ところで V は有限次元だから相異なる重みの数は有限で，十分大きい n について $\mu+nr$ は重みではない．よって $\varphi(e_r)^n V_\mu=\{0\}$ をみたす $n=n(\mu)$ がある．そこで $m=\max\{n_\mu\}$ とおけば $\varphi(e_r)^m=0$ となり (4.22) が証明される．▯

一般体の上に移行する仕組は§4.3 と同様である．L の包絡環を U とする．いま $\mathcal{U}=\sum \boldsymbol{Z}e_{-A}h_Be_C$ とおけば $\mathcal{U}$ は U の $\boldsymbol{Z}$ 形である．また (4.16) により $\mathcal{U}$ は $\boldsymbol{Z}$ 上の多元環となる．定理 4.21 により V は $\mathcal{U}$ 不変な $\boldsymbol{Z}$ 形 $\mathcal{V}$ をもっている．すなわち，$\mathcal{V}$ の基 $\{v_i\}$ をとれば $\{v_i\}$ は $\boldsymbol{C}$ 上でも一次独立で V の基となっている．この基を用いて $\varphi(e_r)^n/(n!)$ の行列表示を考える．

$$\varphi(e_r)^n/(n!)=\varphi(e_r{}^n/(n!)) \qquad (e_r{}^n/(n!)\in\mathcal{U})$$

となるからその行列表示の成分はすべて整数となる（$\mathcal{V}$ が $\mathcal{U}$ 不変）．

さらに $\varphi(e_r)$ はベキ零だから $x_r(\zeta)$ を表わす行列の成分は

$$x_r(\zeta)=\exp \zeta\varphi(e_r)=\sum\zeta^n\varphi(e_r)^n/(n!)$$

より整数係数のζの多項式となる．そこで複素数ζの代りに $\boldsymbol{Z}$ 上の変数 X を代入して $x_r(X)$ を定義すれば $x_r(X)$ は $\boldsymbol{Z}[X]\otimes_{\boldsymbol{Z}}\mathcal{V}$ の $\boldsymbol{Z}[X]$ 加群としての自己準同形である．ところで (4.7) と同様に

$$x_r(X)x_r(-X)=1$$

が成り立つから $x_r(X)$ は可逆元となる．任意の体 F と，F の任意の元 t について $x_r(X)$ の各成分において変数 X に t を代入した行列を $x_r(t)$ とおく．各成分が整数係数の多項式であるから，t を代入したものは F の元として確定した値をもつ．そして $x_r(t)$ は

$$V_F = F \otimes_{\mathbf{Z}} \mathcal{V}$$

の F 線形写像となる．ここでも $x_r(t)x_r(-t)=1$ が成り立つから $x_r(t)$ は可逆な線形写像で

$$\langle x_r(t) \mid r \in \Delta, t \in F \rangle$$

が $GL(V_F)$ の部分群として定義される．$\mathcal{V}$ に別の基 $\{v_i'\}$ をとればこの基ともとの基との間の変換行列は整数成分で行列式の値が ± 1 である．したがって線形写像 $x_r(t)$ は基の取り方にかかわらず同一の写像となる．§4.4 では $\mathcal{V}$ の基をとらずに $x_r(t)$ を定義したがその定義とこの節で述べた定義とが一致することは明らかである．一般の Chevalley 群でも

(4.23)
$$x_r(t_1+t_2) = x_r(t_1)x_r(t_2)$$

が成り立つ．証明は (4.9) と同様であるから省略する．

9. 重みの生成する格子　半単純 Lie 代数 L の Cartan 部分代数を H とする．H の双対空間 H^* の中で L の根が生成する加法群を P とおく．L の根系 Δ の中に基本系 Π を一つ定め

$$\Pi = \{r_1, \cdots, r_l\}$$

とする．任意の根は $r_1, r_2, \cdots, r_l$ の整係数一次結合となるから P は $r_1, \cdots, r_l$ が生成する階数 l の自由加法群である (§1.2)．

§2 において H の元 h_r $(r \in \Delta)$ を定義した．これらの元 h_r が生成する加法群を $\mathcal{H}$ とおく．(2.1) により $\{h_r\}$ は根系をつくり，Π の元に対応する $h_1, h_2, \cdots, h_l$ $(h_i = h_{r_i})$ の集合が根系 $\{h_r\}$ の基本系となる．よって $\mathcal{H}$ は $\{h_r\}$ が生成する階数 l の自由加法群である．

さて根系 Δ の任意の元 r, s について $r(h_s) = n(r, s)$ は整数である．そこで H^* の元 x のうちすべての h_s について $x(h_s) \in \mathbf{Z}$ をみたすもの全体のつくる加法群を Q とおく．

(4.24)　Q の元 q_i $(i=1, 2, \cdots, l)$ を

$$q_i(h_i) = 1, \qquad q_i(h_j) = 0 \quad (j \neq i)$$

と定義すれば Q は $q_1, q_2, \cdots, q_l$ が生成する自由加法群である．

証明　$\{h_i\}$ は基本系だから任意の h_r は $h_1, \cdots, h_l$ の整数係数一次結合となる．したがって Q の元は $q_1, \cdots, q_l$ の整数係数一次結合となる．$q_1, \cdots, q_l$ が Q の自由生成元であることは明らかである．□

定義 4.25 L 加群 V による L の表現を φ とおく．V における表現の重み全体が生成する加法群を**重み**の生成する**格子**といい Γ_V または Γ_φ と表わす．上に定義した群 Q を**重み加群**という．□

φ が随伴表現の場合 $\Gamma_\varphi=P$ となる．一般に φ による一般 Chevalley 群の構造は Γ_φ によって定まることが後章で証明される(定理 8.3)．

(4.26) 任意の忠実な表現 φ について $Q\supset\Gamma_\varphi\supset P$ が成り立つ．特に φ の任意の重み μ について $\mu(h_s)$ は整数である．

証明 $V=V_1\oplus V_2$ と L 加群として直和分解していると仮定しよう．いま μ を重みとし $v\neq 0$ を V_μ の元とする．任意の $h\in H$ に対し

$$hv=\mu(h)v$$

が成り立つ．いま $v=v_1+v_2$ $(v_i\in V_i)$ と分解すれば $v_1\neq 0$ または $v_2\neq 0$ となる．明らかに $hv_i=\mu(h)v_i$ $(i=1,2)$ が成り立つから μ は V_1 または V_2 の重みとなる．

V の任意の重み μ について $\mu(h_r)$ が整数であることを証明しよう．半単純 Lie 代数の表現は完全可約だから V が既約 L 加群の場合に証明すればよい．そこで V が既約と仮定すれば (4.20) により重みは $\mu=\Lambda-\sum m_r r$ という形をしている．ここで Λ は最高重みで $m_r\in\boldsymbol{Z}$ となる．(4.19)により Λ は h_r で整数値をとるから $\mu(h_r)\in\boldsymbol{Z}$ を得る．すなわち $Q\supset\Gamma_\varphi$ となる．

次に $\Gamma_\varphi\supset P$ を証明しよう．(4.22)の証明で注意したように $V=\sum V_\mu$ が成り立つ．さて r を任意の根とすれば L の作用は忠実だから $e_rV\neq\{0\}$ を得る．したがって少なくとも一つの重み μ について $e_rV_\mu\neq\{0\}$ が成り立つ．ところで (4.18) により $e_rV_\mu\subset V_{\mu+r}$ だから $\mu+r$ は V の重みとなる．よって $r=(\mu+r)-\mu\in\Gamma_\varphi$ を得る．すなわち，$\Gamma_\varphi\supset P$ が成り立つ．□

注意 (4.20) のあとで述べた存在定理により Q の元 q_i を最高の重みとする既約表現が存在する．その直和をつくれば $\Gamma_\varphi=Q$ を満足する表現の存在することがわかる．□

§5 古典型 Chevalley 群

1. 自然表現と随伴表現　§3において古典型複素単純 Lie 代数について述べた．それらはある種の行列の集合で括弧積に関して閉じている体系として定義されている．この節では類似の関係が Chevalley 群についても成り立つこ

とを証明しよう．古典型の群は第2章で述べた古典群と同形になるのである．

いま L を古典型複素単純 Lie 代数とし，L に対応する根系を Δ とおく．L は線形空間 V の線形写像のつくる Lie 代数と考えられるから，V に基

$$\{y_1, y_2, \cdots, y_n\}$$

を定めこの基によって L の元の行列表示が得られているとする．

さて L の Chevalley の標準基 B を§3で定めた通りとする．B の各元の行列表示の成分はすべて整数であることに注意しよう．そこで

$$\mathcal{V}=\boldsymbol{Z}y_1+\boldsymbol{Z}y_2+\cdots+\boldsymbol{Z}y_n$$

とおけば $\mathcal{V}$ は V の $\boldsymbol{Z}$ 形であるがこれが定理4.21における許容 $\boldsymbol{Z}$ 形であることを示そう．B の元 e_r は V の線形写像であるが $\mathcal{V}$ を不変にしているから，$\mathcal{V}$ の $\boldsymbol{Z}$ 線形写像と考えることができる．そこで e_r は

$$V_F=F\otimes_{\boldsymbol{Z}}\mathcal{V}$$

に F 線形写像 $1\otimes e_r$ を定める．§4.3のように $1\otimes e_r$ を略式に e_r と表わすことにする．

(5.1)　任意の体 F と，F の元 t をとる．$\Delta\neq B_l$ ならば任意の $r\in\Delta$ について $(te_r)^2=0$ が成り立つ．$\Delta=B_l$ の場合でも§3の記号で $r\neq\pm e_i$ ならば $(te_r)^2=0$ となる．しかし $r=\pm e_i$ の場合は

$$(te_r)^2=2t^2e,\quad (te_r)^3=0$$

が成り立つ．ここで e は $\mathcal{V}$ の $\boldsymbol{Z}$ 線形写像であって次式で与えられる．

$$r=e_i \Longrightarrow e=-e_{i,l+i}$$

$$r=-e_i \Longrightarrow e=-e_{l+i,i}.$$

証明　おのおのの場合に計算を実行してみれば(5.1)の成り立っていることがわかる．□

(5.1)により $\mathcal{V}$ が許容 $\boldsymbol{Z}$ 形であることは明らかである．そこで L の V 上の自然な表現 φ による Chevalley 群を考え，その生成元 $x_r(t)$ を書き上げてみよう．$(te_r)^2=0$ ならば

$$x_r(t)=1+te_r$$

となる．ここで最初の1は V_F の恒等写像を表わす．$(te_r)^2\neq 0$ ならば

$$x_r(t)=1+te_r+t^2e$$

となっている．

Lie 代数 L を随伴表現 ad により L の上に作用させれば §4.3 において定義した Chevalley 群が得られる．この群と自然表現による Chevalley 群との関係を調べてみよう．複素数体の上で随伴表現による Chevalley 群の生成元は $\exp(\zeta \operatorname{ad} e_r)$ で L の元 x に次の様に作用している(定理 4.4 参照)．

$$\exp(\zeta \operatorname{ad} e_r)x=\exp(\zeta e_r)x(\exp \zeta e_r)^{-1}.$$

この右辺における $\exp \zeta e_r$ は自然表現による Chevalley 群の生成元 $x_r(\zeta)$ と一致する(5.1)．同様の結果が任意の体の上で成り立つ．

定理 5.2　L を古典型単純 Lie 代数とする．任意の体 F 上で随伴表現による Chevalley 群の生成元を $x_r(t)$ と表わす．この時，任意の $u\in L_F$ に対し

$$x_r(t)u=e(r,t)ue(r,t)^{-1}$$

となる．ここで $e(r,t)=1+te_r+t^2e$ は自然表現による Chevalley 群の生成元と一致する．(e は B_l 型かつ $r=\pm e_i$ の時 (5.1) で定めた通り，その他の場合は $e=0$ とおく．)

証明　$r\in\Delta$ を一つ定める．変数 T をとり整係数多項式環を $\boldsymbol{Z}[T]$ とおく．いま $\boldsymbol{Z}[T]\otimes_{\boldsymbol{Z}}\mathscr{V}$ の $\boldsymbol{Z}[T]$ 線形写像 $e(T)$ を

$$e(T)=1+Te_r+T^2e$$

とおく．(4.7) の証明と同様に $e(T)e(-T)=1$ が得られる．よって $e(T)$ は可逆である．さて標準基 B の元 u を一つ定めしばらくの間，動かさないことにする．元 $e(T)ue(T)^{-1}$ は $\boldsymbol{Z}[T]$ の元を成分とする行列だから

$$e(T)ue(T)^{-1}y_i=\sum P_{ij}(T)y_j \qquad (P_{ij}(T)\in\boldsymbol{Z}[T])$$

とおくことができる．また $x_r(T)$ を (4.7) の証明において定義したものとすれば $x_r(T)u\in\boldsymbol{Z}[T]\otimes\mathscr{L}$ となる．したがって

$$x_r(T)uy_i=\sum Q_{ij}(T)y_j \qquad (Q_{ij}(T)\in\boldsymbol{Z}[T])$$

を得る．よって任意の複素数 ζ について

$$x_r(\zeta)uy_i=\sum Q_{ij}(\zeta)y_j$$

$$e(\zeta)ue(\zeta)^{-1}y_i=\sum P_{ij}(\zeta)y_j$$

が成り立つ．ところで $e(\zeta)=\exp(\zeta e_r)$ だから定理 4.4 により

$$P_{ij}(\zeta)=Q_{ij}(\zeta)$$

がすべての $\zeta\in\boldsymbol{C}$ について成り立つ．したがって多項式として $P_{ij}(T)=Q_{ij}(T)$ となる．F の元 t を代入すれば定理 5.2 の正しいことがわかる．　□

随伴表現による Chevalley 群は L_F の自己同形のつくる群として定義された(定義4.10). 古典型の場合この群は自然表現による Chevalley 群が引きおこす内部自己同形のつくる群と一致する.

2. A_l 型の Chevalley 群 A_l 型の複素単純 Lie 代数 L は対角和が0の (n,n) 型の行列 $(n=l+1)$ 全体のつくる Lie 代数である. §3.1により

$$B=\{e_{ii}-e_{i+1,i+1}, e_{ij}\ (i\neq j)\}$$

が Chevalley の標準基となる. よって任意の体 F について L_F はやはり対角和が0の (n,n) 型行列の全体と一致する.

自然表現による Chevalley 群は

$$x_r(t)=1+te_{ij} \qquad (r=e_i-e_j)$$

が生成する $GL(V)$ の部分群である. よって定理 II 2.7により次の命題を得る.

定理 5.3 自然表現による A_l 型 Chevalley 群は $SL(l+1,F)$ と同形である.

この定理から随伴表現による群も決定される.

(5.4) 随伴表現による A_l 型 Chevalley 群は $SL(l+1,F)$ の中心による商群 $PSL(l+1,F)$ と同形である.

証明 $SL(n,F)$ の元 $\sum\alpha_{ij}e_{ij}$ が L_F の各元と可換ならば

$$(\sum\alpha_{ij}e_{ij})e_{kl}=e_{kl}(\sum\alpha_{ij}e_{ij})$$

がすべての $k,l\ (k\neq l)$ について成り立つ. よって $\alpha_{lj}=0\ (l\neq j), \alpha_{ll}=\alpha_{kk}$, すなわち $SL(n,F)$ の引きおこす内部自己同形の群は $PSL(n,F)$ である. ▯

3. B_l 型の Chevalley 群 議論を簡単にするため係数体の標数は2でないと仮定する. B_l 型の複素単純 Lie 代数は $L=L(J_B)$ という形をしている(§3.2). 標準基の取り方からわかる様に L_F も $L(J_B)$ という形である. すなわち L_F の元 u は ${}^tuJ_B+J_Bu=0$ をみたしている. さて自然表現による Chevalley 群の生成元は

$$x_r(s)=1+se_r+(se_r)^2/2$$

である. 体 F の標数は2ではないから分母に2があってもかまわない. se_r は L_F の元だから ${}^t(se_r)J_B=-J_B(se_r)$ をみたしている. よって

$${}^t(x_r(s))J_B=J_Bx_r(-s)=J_Bx_r(s)^{-1}$$

が成り立つ．これは $x_r(s)$ が J_B に対応する対称形式 f を不変にしていることを示している（I §4）．そこで f を同伴形式とする2次形式を Q とおけば，自然表現による B_l 型 Chevalley 群は直交群 $O(Q)$ の部分群である．また f の形から Q の指数は最大値 l となっていることがわかる．

§3.2の記号を用い

$$V_i(t)=1+tv_i-t^2e_{i,l+i}$$
$$U_i(t)=1+tu_i-t^2e_{l+i,i}$$

さらに $U_{ij}(t)=1+tu_{ij}, S_{ij}(t)=1+ts_{ij}, T_{ij}(t)=1+tt_{ij}$ とおく．ここで $v_i, u_i, u_{ij}, s_{ij}, t_{ij}$ は §3.2 で定義した元である．さて

$$[U_i(s), V_j(t)]=U_{ji}(-2st)$$
$$[V_i(s), V_j(t)]=S_{ij}(-2st)$$
$$[U_i(s), U_j(t)]=T_{ij}(2st)$$

が成り立つ．V の基を $\{y_0, y_1, \cdots, y_{2l}\}$ とすれば J_B の形から y_0+ty_i が非特異元となる．そこで y_0+ty_i に関する対称変換を S_i，y_0 に関する対称変換を S_0 とおけば（行列表示を計算すればわかるように）

$$V_i(t)=S_iS_0$$

が成り立つ．同様に y_0-ty_{l+i} に関する対称変換を S_{l+i} とおけば

$$U_i(t)=S_{l+i}S_0$$

となる．また $Q(y_0)=Q(y_0+ty_i)=Q(y_0-ty_{l+i})=1$ だから $V_i(t)$ も $U_i(t)$ もスピンノルムが1となり $O(Q)$ の交換子群に含まれている（II (9.6)参照）．よって自然表現による B_l 型の Chevalley 群は $O(Q)$ の交換子群 $\Omega(Q)$ に含まれている．実際この群は $\Omega(Q)$ と一致する．節末の注意を参照されたい．

4. C_l 型の Chevalley 群 ($l\geqq 3$)　この場合 J_C に対応する形式は非退化交代形式である．B_l 型の場合と同様に自然表現による Chevalley 群は斜交群 $Sp(2l, F)$ に含まれていることがわかる．次の定理が成り立つ．

定理 5.5 自然表現による C_l 型 Chevalley 群 ($l\geqq 3$) は斜交群と一致する．随伴表現による群は $PSp(2l, F)$ と同形である．

証明 自然表現による C_l 型 Chevalley 群を G とおく．§3.3における標準基の元の形からわかるように，$\det A=1$ を満足する (l,l) 型の行列 A および (l,l) 型対称行列 B に対して

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{pmatrix}, \quad \begin{pmatrix} I & B \\ 0 & I \end{pmatrix}, \quad \begin{pmatrix} I & 0 \\ B & I \end{pmatrix}$$

という形の行列はすべて G に含まれている．まず G が $V_F-\{0\}$ の上に可移に作用していることを示そう．V の自然な基 $\{y_i\}$ をとり V_F の元 $w \neq 0$ を表わした時その前半，すなわち $y_1, \cdots, y_l$ の一次結合となっている部分を u とおき，後半を v とする．もし $v=0$ ならば適当に A をとれば u を y_1 にうつすことができる(I (2.11))．もし $v \neq 0$ ならば v を y_{l+1} にうつすことができる．さらに G の元 $I+ts_{1j}$ を用いれば u における y_j の係数に t を加えることができる．よって G は w を λy_1+y_{l+1} に移す元を含んでいる．

さて $I-\lambda e_{1,l+1} \in G, I-e_{l+1,1} \in G$ である．そこで

$$(I-e_{l+1,1})(I-\lambda e_{1,l+1})(\lambda y_1+y_{l+1})=y_1$$

を得るから G は $V_F-\{0\}$ に可移に作用する．

元 y_1 に関する斜交移換 $\tau_1=\tau(t, y_1)$ を基 $\{y_i\}$ を用いて行列表現してみれば $I+\lambda e_{1,l+1}$ となる．よって τ_1 は G に含まれている．

さて $\tau=\tau(t,a)$ を任意の斜交移換とすれば $\sigma(a)=y_1$ をみたす G の元 σ がある．よって $\sigma\tau\sigma^{-1}=\tau(t, y_1)$ は y_1 に関する斜交移換となるから $\sigma\tau\sigma^{-1} \in G$, したがって $\tau \in G$ となる．このように G はすべての斜交移換を含むから定理 II 5.3 により $G=Sp(2l, F)$ を得る．

随伴表現による C_l 型の Chevalley 群は $Sp(2l, F)$ の元が L_F にひきおこす共役写像のつくる群である．L_F のすべての元と可換な斜交群の元は $\pm I$ しかないことが定理 II 5.5 と同様に証明される．したがって随伴表現による群は

$$Sp(2l, F)/\{\pm I\}=PSp(2l, F),$$

つまり射影斜交群と同形である．□

5. D_l 型の Chevalley 群 ($l \geqq 4$)　　自然表現による D_l 型 Chevalley 群を G とおく．D_l 型の場合 J_D は対称形式に対応しているが F の標数が 2 の場合も含めるため 2 次形式を考える．そこで

$$Q(\sum \lambda_i y_i)=\lambda_1\lambda_{l+1}+\lambda_2\lambda_{l+2}+\cdots+\lambda_l\lambda_{2l}$$

とおけば Q は指数 l の 2 次形式である．G の生成元 $x_r(t)$ は

$$I+tu_{ij}, \quad I+ts_{ij}, \quad I+tt_{ij}$$

のいずれかに等しい(§3.4 参照)．各生成元が Q を不変にしていることを容易

に確かめることができる．たとえば $I+tu_{ij}$ は

$$\lambda_i\lambda_{l+i}\to\lambda_i(\lambda_{l+i}-t\lambda_{l+j}),\quad \lambda_j\lambda_{l+j}\to(\lambda_j+t\lambda_i)\lambda_{l+j}$$

その他の $\lambda_k\lambda_{l+k}$ は変わらない．よって $I+tu_{ij}$ は Q を不変にする．他の生成元についても同様であるから G は直交群 $O(Q)$ の部分群となる．以下 G が $O(Q)$ の交換子群と一致することを証明しよう．

G の元を行列で書けば $\langle I+tu_{ij}\ (i\neq j)\rangle$ は

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{pmatrix} \qquad (A\in SL(l,F))$$

という形の行列群である(定理 II 2.7)．ここで $I+tu_{ij}$ に対応する元では $A=I+te_{ij}$ となり移換である．$l\geqq 4$ だから定理 II 2.5 により $I+tu_{ij}$ は G の中で交換子となっている．

他の生成元についてもそれが交換子であることを直接証明することもできるが次の様に考えてもよい．V_F の元 y_i+y_{l+i} は非特異だからそれに関する対称変換 σ の行列を S とおく．S による共役写像で G の生成元の集合が不変になることを示そう．さて $\sigma(y_i)=-y_{l+i}, \sigma(y_{l+i})=-y_i$ でその他の基の元は不変となる．よって $S(I+tu_{ij})S^{-1}\ (i\neq j)$ は $I\pm tt_{ij}$ となる．同様に $S(I+tu_{ji})S^{-1}$ は $I\pm ts_{ij}$ となり $k\neq i, l\neq i$ ならば S は $I+tu_{kl}$ などと可換である．したがって S による共役写像は G を不変にする．すなわち G の自己同形を引きおこしている．上のことから G の生成元はすべて交換子となることがわかる．よって G は $O(Q)$ の交換子群 $\Omega(Q)$ に含まれている．

次に V の非特異元 y を任意にとれば G の元 σ があって

$$\sigma(y)=y_1+\lambda y_{l+1} \qquad (\lambda=Q(y))$$

とできることを証明しよう．y を $\{y_1,\cdots,y_{2l}\}$ の一次結合として

$$y=\sum\lambda_iy_i$$

と表わせば $Q(y)\neq 0$ だから $\lambda_1y_1+\cdots+\lambda_ly_l\neq 0$ でなければならない．前に述べた様に G は

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{pmatrix} \qquad (A\in SL(l,F))$$

という形の行列を全部含んでいるから I (2.11) により $\sigma_1\in G$ を適当に選んで

$$\sigma_1y=y_1+\sum\mu_iy_{l+i}$$

とすることができる．この両辺に $\sigma_i=I-\mu_i t_{1i}$ $(i>1)$ を作用させれば y_{l+i} の係数が 0 となる．よって $\sigma=\sigma_l\cdots\sigma_2\sigma_1$ により y は $y_1+\lambda y_{l+1}$ に移る．

さて $\lambda\neq 0$ ならば $y_1+\lambda y_{l+1}$ は非特異元である．そこで $y_1+\lambda y_{l+1}$ に関する対称変換を σ_λ とおく．この時

$$O(Q)=\langle G, \sigma_\lambda\ (\lambda\in F^{\#})\rangle$$

が成り立つことを証明しよう．いま任意の対称変換を ρ とする．ρ はある非特異元 y に関する対称変換である．上に証明したように G の元 σ があって $\sigma(y)=y_1+\lambda y_{l+1}$ となる．よって $\sigma\rho\sigma^{-1}=\sigma_\lambda$ が成り立つ．すなわち，任意の対称変換 ρ は $\langle G, \sigma_\lambda\rangle$ に含まれている．この場合 $l\geqq 4$ だから定理 II 7.18 により $O(Q)=\langle G, \sigma_\lambda\rangle$ となる．

前と同様に $\sigma_\lambda(y_1)=-\lambda y_{l+1}, \sigma_\lambda(y_{l+1})=-\lambda^{-1}y_1$ が成り立つ．よって σ_λ による共役写像により G の生成元の集合が不変になる．すなわち

$$G\lhd O(Q)$$

が成り立つ．そこで $H=\langle\sigma_\lambda\ (\lambda\in F^{\#})\rangle$ とおけば

$$O(Q)=GH,\quad O(Q)/G=H/H\cap G$$

となる．σ_λ は y_1, y_{l+1} が生成する強双曲型平面の直交群に含まれている．そこで $K=\langle\sigma_\lambda\sigma_\mu\rangle$ とおけば K は可換群である．II §9 で述べた様に直交群 $O(Q)$ は指数 2 の部分群 $\varphi(G^+)$ を含んでいる(定理 II 9.2 (iv))．II (9.5) によれば G^+ の各元は偶数個の V の非特異元の積であるから $\varphi(G^+)$ の元は偶数個の対称変換の積である(定理 II 9.2(i) 参照)．よって

$$GK=\varphi(G^+)$$

となる．($|H:K|=2$ である．) よって $\varphi(G^+)/G=K/K\cap G$ は可換群である．このように G は $\varphi(G^+)$ の交換子群を含んでいる．ところで定理 II 9.8 により $\varphi(G^+)$ の交換子群は $\Omega(Q)$ と一致する．すなわち $\Omega(Q)\subset G$ となる．$G\subset\Omega(Q)$ を前に証明したから $G=\Omega(Q)$ が成り立つ．

随伴表現による群を決めるため G の元 ρ が L_F の各元と可換だとすれば，前と同様 $\rho=\pm I$ となる．よって随伴表現による D_l 型の Chevalley 群は

$$\Omega(Q)/\{\pm I\}\quad \text{または}\quad \Omega(Q)$$

となる．すなわち次の定理が証明された．

定理 5.6　自然表現による D_l 型 Chevalley 群は $2l$ 次元の空間における指

数 l の 2 次形式 Q に関する直交群の交換子群 $\Omega(Q)$ と一致する．随伴表現による群は $-I\in\Omega(Q)$ または $-I\notin\Omega(Q)$ に応じて

$$\Omega(Q)/\{\pm I\} \quad \text{または} \quad \Omega(Q)$$

と同形になる． □

注意 1. B_l 型 $(l\geqq 2)$ の Chevalley 群 G も D_l 型と同様に直交群の交換子群 $\Omega(Q)$ と同形であることを証明することができる．まず任意の非特異元を $y_1+\lambda y_{l+1}$ に移す G の元が存在することを証明する．適当に $V_i(t), U_i(s)$ を用いれば y_0 の係数を 0 にすることができるから D_l の場合に帰着される．あとは D_l の場合と全く同様に $G=\Omega(Q)$ が証明される．この場合も L_F の各元と可換な G の元は $\pm I$ に限るが V の次元が奇数だから $-I\notin\Omega(Q)$．したがって随伴表現の場合も B_l 型の Chevalley 群は $\Omega(Q)$ である．

注意 2. D_l 型の場合 $-I\in\Omega(Q)$ となるための条件は $(-1)^l$ が F の平方元となることである．これを証明するに当って F の標数は 2 でないと仮定することができる．定理 II 3.4 により V は直交基 $\{v_i\}$ をもつ．そこで v_i に関する対称変換を σ_i とおけば $\sigma_i(v_i)=-v_i$ であるが他の元 v_j は動かさない．よって $-I=\sigma_1\sigma_2\cdots\sigma_n$ $(n=2l)$ となる．さて II (9.6) により $-I$ のスピンノルムは $(F^*)^2$ を法として $\prod Q(v_i)$ と合同となる．ところで $2^n\prod Q(v_i)$ は Q の判別式である．Q の指数が l だから Q の判別式は $(F^*)^2$ を法として $(-1)^l$ に合同となる（V は強双曲型）．したがって II §9 の結果から

$$-I\in\Omega(Q)\Longleftrightarrow(-1)^l\in(F^*)^2$$

を得る．F が有限体の場合 $|F|=q$ が奇数とすれば

$$-I\in\Omega(Q)\Longleftrightarrow l \text{ が偶数，または } l \text{ が奇数で } q\equiv 1 \pmod 4$$

となる．この条件は $q^l\equiv 1 \pmod 4$ とまとめることもできる． □

§6 複素 Chevalley 群

1. 準備 この節では複素数体上の一般 Chevalley 群の構造を調べ，生成元の間に成り立っているいくつかの関係式を導く．これらの関係式は一般体の上の Chevalley 群を調べるに当って基本となるものである．この節では係数体は複素数体に限るから特にことわらない．

(6.1) 線形空間 V の線形写像 α,β に対し $[\alpha,\beta]=\alpha\beta-\beta\alpha$ を γ とおく．もし γ が α および β と可換ならば

$$\exp(\alpha+\beta)=(\exp\ \alpha)(\exp\ \beta)(\exp(-\gamma/2))$$

が成り立つ．

証明 帰納法により $\beta\alpha^i=\alpha^i\beta-i\alpha^{i-1}\gamma$ を得る．さて

(6.2) $$(\alpha+\beta)^n/n!=\sum\alpha^i\beta^j(-\gamma)^k/i!\,j!\,2^kk!,$$

ここで右辺の和は $i+j+2k=n$ をみたす非負整数の三つ組 (i,j,k) 全体にわたる和であることを n に関する帰納法で証明しよう．いま (6.2) が n について成り立つと仮定すれば

$$(\alpha+\beta)^{n+1}/(n+1)!=\sum(\alpha+\beta)\alpha^i\beta^j(-\gamma)^k/i!j!2^kk!(n+1)$$

となる．この右辺の各項に $\beta\alpha^i=\alpha^i\beta-i\alpha^{i-1}\gamma$ を用いれば右辺が3組の和に分かれる．そこで $a+b+2c=n+1$ をみたす非負整数の組を一つ定めれば各和から $\alpha^a\beta^b(-\gamma)^c/a!b!2^cc!$ が現われる．その係数の和が

$$(a/n+1)+(b/n+1)+(2c/n+1)=1$$

となり，帰納法により(6.2)が成り立つ．そこで(6.2)の両辺を n について加えれば右辺では i,j,k について別々に加えることができて(6.1)が証明される． □

(6.3) L を半単純 Lie 代数とし V を忠実な L 加群とする．V による L の表現を φ とおき $x_r(\zeta)$ を表現 φ による一般 Chevalley 群の生成元の一つとする．任意の元 $y\in L$ について

$$x_r(\zeta)\varphi(y)x_r(\zeta)^{-1}=\varphi(\exp(\zeta\ \mathrm{ad}\ e_r)y)$$

が成り立つ．

証明 記号を簡単にするために $\zeta e_r=x$ とおく．(4.6) および (4.22) により ad x および $\varphi(x)$ は共にベキ零である．そこで

$$(\mathrm{ad}\ x)^m=0,\quad \varphi(x)^m=0$$

をみたす自然数 m を一つ定めておく．任意の n について（定理4.4参照）

$$(\mathrm{ad}\ x)^ny/n!=\sum(x^k/k!)y((-x)^{n-k}/(n-k)!)$$

が成り立つ．この右辺は L の包絡環の元として定まっている．この両辺を n について0から N まで加える．ここで $N\geqq 2m$ とすれば左辺の和は

$$(\exp\ \mathrm{ad}\ x)y$$

に一致する．そこで両辺の φ による像をとれば（φ は包絡環の表現に拡張されるから(4.14)）

$$\varphi(\exp \mathrm{ad}\ x)y=\sum_n\sum_k(\varphi(x)^k/k!)\varphi(y)((-\varphi(x))^{n-k}/(n-k)!)$$

を得る．この右辺の和では $k\leqq m$ の範囲でよい．さて右辺の和の順序をかえればまず n について $n=k$ から N までの和をとることになる．よって最後の項を $n-k=0$ から $N-k$ まで加えるが $k\leqq m, N\geqq 2m$ だから

$$N-k\geqq N-m\geqq m$$

となりこの和は $\exp(-\varphi(x))=x_r(-\zeta)$ に一致する．よって

$$\varphi(\exp \mathrm{ad}\, x)y=x_r(\zeta)\varphi(y)x_r(\zeta)^{-1}$$

が成り立つ． □

注意 (6.3) において右辺は §4 の記号では $\varphi(x_r(\zeta)y)$ と一致する．このように一般 Chevalley 群の生成元は随伴表現の場合の生成元と密接に結び付いている．定理 5.2 参照． □

2. Chevalley の公式 L を複素半単純 Lie 代数とし，その忠実な表現を φ，φ に対応する表現加群を V とおく．表現 φ による一般 Chevalley 群を

$$\langle x_r(\zeta)\,|\,r\in\Delta, \zeta\in \boldsymbol{C}\rangle$$

とすれば次の Chevalley の公式が成り立つ．

定理 6.4 任意の根 r,s をとり $s\neq\pm r$ と仮定すれば

$$x_r(\zeta)x_s(\eta)x_r(\zeta)^{-1}=x_s(\eta)\prod x_{ir+js}(C_{ijrs}\zeta^i\eta^j)$$

が成り立つ．右辺は $i>0, j>0, ir+js\in\Delta$ をみたす組 (i,j) についての積でその順序は $i+j$ が増加する順にとる．係数 C_{ijrs} は整数で ζ,η には無関係に定まる．さらに

$$C_{i1rs}=M_{r,s,i},\quad C_{1jrs}=(-1)^jM_{s,r,j}$$

が成り立つ．ここで $M_{r,s,i}$ は (4.6) で定義された整数である．

証明 $y=\eta e_s$ とおけば (6.3) より

$$x_r(\zeta)(\varphi(y)^n/n!)x_r(\zeta)^{-1}=\varphi((\exp \mathrm{ad}\,\zeta e_r)y)^n/n!$$

を得る．定理 6.4 の公式の左辺を C とおけば $C=\exp\varphi((\exp \mathrm{ad}\,\zeta e_r)y)$ となる．(4.6) により ($x_r(\zeta)e_s$ の式から)

$$C=\exp(\eta\varphi(e_s)+\sum M_{r,s,i}\zeta^i\eta\varphi(e_{ir+s}))$$

と書ける．もし $r+s\notin\Delta$ ならば上式は $C=\exp(\varphi(\eta e_s))$ となり定理が成り立つ．さて (1.4) により r,s は 2 次元の根系を生成する．まず $ir+js\in\Delta\Rightarrow j=1$ が成り立つ場合を考えよう．この時 e_{ir+s} $(i=1,2,\cdots)$ は互いに交換可能だから (4.2) が適用され

$$C=x_s(\eta)\prod x_{ir+s}(M_{r,s,i}\zeta^i\eta)$$

となる．よってこの場合，定理が成り立つ．

次に r,s が B_2 型の根系を生成するとしよう．$r+2s$ が根ならば s が短い根で $[e_s,e_{r+s}]=N_{s,r+s}e_{r+2s}$ となる．よって

$$C=\exp(\eta\varphi(e_s)+N_{r,s}\zeta\eta\varphi(e_{r+s}))$$

の右辺に (6.1) が適用される. $N_{r,s}N_{s,r+s}=-2M_{s,r,2}$ を用いて

$$C=x_s(\eta)x_{r+s}(N_{r,s}\zeta\eta)x_{r+2s}(M_{s,r,2}\zeta\eta^2)$$

を得る. よってこの場合も定理が成り立つ.

残りの場合には r, s が G_2 型の根系を生成する. $ir+2s\in\Delta$ とすれば三つの場合のうち一つがおこる. まず $r+2s\in\Delta, r+3s\notin\Delta$ とすれば r, s は共に短い根で e_{r+2s}, e_{2r+s} は共に e_r とも e_s とも交換可能である. したがって (6.1) が適用され C は

$$\exp(\eta\varphi(e_s)+N_{r,s}\zeta\eta\varphi(e_{r+s}))x_{2r+s}(M_{r,s,2}\zeta^2\eta)$$
$$=x_s(\eta)x_{r+s}(N_{r,s}\zeta\eta)x_{r+2s}(M_{s,r,2}\zeta\eta^2)x_{2r+s}(M_{r,s,2}\zeta^2\eta)$$

となる. 次に $r+2s\notin\Delta, 3r+2s\in\Delta$ とすれば r が短い根, s は長い根で e_r も e_s も e_{3r+2s} と交換可能である. この場合も (6.1) が適用され

$$C=x_s(\eta)\prod x_{ir+s}(M_{r,s,i}\zeta^i\eta)x_{3r+2s}(A\zeta^3\eta^2)$$

を得る. ここで A が整数 (±1 または ±2) であることを証明しよう. (2.6) により $M_{r,s,i}=\pm1, N_{s,3r+s}=\pm1, N_{r+s,2r+s}=\pm3$ となる. よって (6.1) に従って交換子を計算すれば

$$A=-(1/2)(M_{r,s,3}N_{s,3r+s}+N_{r,s}M_{r,s,2}N_{r+s,2r+s})$$

を得る. 括弧の中の第1項は ±1, 第2項は ±3 だから A は整数となる.

最後に $r+2s\in\Delta, r+3s\in\Delta$ とすれば $(s, s)<(r, r)$ となる. この場合は (6.1) が適用できないので次の様に考える. r と s とを入れ替えれば前に証明した場合となるから

$$x_s(\eta)x_r(\zeta)x_s(\eta)^{-1}=x_r(\zeta)\prod x_{r+is}(M_{s,r,i}\zeta\eta^i)x_{2r+3s}(B\zeta^2\eta^3)$$

が成り立つ. ここで η を $-\eta$ に変えれば

$$C=x_s(\eta)x_r(\zeta)\prod x_{r+is}(M_{s,r,i}\zeta(-\eta)^i)x_{2r+3s}(-B\zeta^2\eta^3)x_r(\zeta)^{-1}$$

を得る. ところで $2r+is\in\Delta$ は $i=3$ の時に限るから $x_r(\zeta)$ は x_{r+3s} 項以外とは可換で,

$$C=x_s(\eta)\prod x_{r+is}((-1)^iM_{s,r,i}\zeta\eta^i)x_{2r+3s}(A'\zeta^2\eta^3)$$

となる. ここで $A'=-M_{s,r,3}N_{r,r+3s}-B$ は整数である. よってすべての場合に定理の成り立つことが証明された. □

3. 単項型の元 前節に引続き表現 φ による一般 Chevalley 群を考え, そ

の生成元を $x_r(\zeta)=\exp \zeta\varphi(e_r)$ と表わす.

定義 6.5 任意の $r\in\Delta$ と $\zeta\in C^*$ について

$$\omega_r(\zeta)=x_r(\zeta)x_{-r}(-\zeta^{-1})x_r(\zeta)$$
$$h_r(\zeta)=\omega_r(\zeta)\omega_r(-1)$$

とおく. $\omega_r(1)$ を略して ω_r と表わすことにする. $\omega_r(\zeta)$ を**単項型**の元という.

注意 L として A_1 型の単純 Lie 代数をとればその自然表現による群では生成元 $x_r(\zeta), x_{-r}(\eta)$ はそれぞれ

$$\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix},\qquad \begin{pmatrix}1 & 0\\ \eta & 1\end{pmatrix}$$

という行列に対応している(§5.2). この場合 $\omega_r(\zeta)$, $h_r(\zeta)$ は

$$\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ -\zeta^{-1} & 1\end{pmatrix}\begin{pmatrix}1 & \zeta\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & \zeta\\ -\zeta^{-1} & 0\end{pmatrix}$$
$$\begin{pmatrix}0 & \zeta\\ -\zeta^{-1} & 0\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}\zeta & 0\\ 0 & \zeta^{-1}\end{pmatrix}$$

に対応する. $h_r(\zeta)$ は Chevalley 群の元である. これと前に定義した元 h_r と混同しないように注意しておく. ▯

(6.6) φ が随伴表現ならば $\omega_r(\zeta)$ は L の自己同形であって

$$\omega_r(\zeta)h_s=w_r(h_s)=h_t \qquad (t=w_r(s))$$

が成り立つ. ここで w_r は r に関する対称変換である.

証明 φ が随伴表現ならば $x_r(\zeta)$ は(4.6)で定義した L の自己同形と一致する. よって (4.6) の式 (*) により作用が定まっている. そこで式 (*) と定義 6.5にしたがって $\omega_r(\zeta)h_s$ を計算すれば

$$\omega_r(\zeta)h_s=h_s-n(r,s)h_r$$

となる. この右辺は $w_r(h_s)=h_t$ $(t=w_r(s))$ に等しい. ▯

φ が一般の場合上の結果に対応するのは次の命題である.

(6.7) 表現 φ を任意にとる. φ による一般 Chevalley 群で

$$\omega_r(\zeta)\varphi(h_s)\omega_r(\zeta)^{-1}=\varphi(h_t) \qquad (t=w_r(s))$$

が成り立つ.

証明 前に注意したように (6.3) の公式を

$$x_r(\zeta)\varphi(y)x_r(\zeta)^{-1}=\varphi(x_r(\zeta)y)$$

と書くことができる. この右辺の $x_r(\zeta)$ は随伴表現による Chevalley 群の元である. この記法を用いれば

$$\omega_r(\zeta)\varphi(h_s)\omega_r(\zeta)^{-1}=\varphi(\omega_r(\zeta)h_s)$$

となる．(6.6) によりこの右辺は $\varphi(h_t)$ に等しい． □

(6.8) 任意の L 加群を V とし V による表現を φ とおく．V の許容 $\boldsymbol{Z}$ 形を $\mathcal{V}$，φ の重みの一つを μ とする．任意の根 r について $\lambda=w_r(\mu)$ とおけば λ は φ の重みとなる．$\mathcal{V}_\mu$ の元 $v\neq 0$ に対し

$$\omega_r(\zeta)v=\zeta^{-m}v'$$

をみたす $\mathcal{V}_\lambda$ の元 v' が存在する．ここで v' は ζ に無関係に r と v だけで定まる元で $m=\mu(h_r)$ である．

証明 (6.7) により任意の $v\in\mathcal{V}_\mu$ について

$$\varphi(h_t)\omega_r(\zeta)v=\omega_r(\zeta)\varphi(h_s)v=\mu(h_s)\omega_r(\zeta)v$$

が成り立つ．そこで $v\neq 0$ ならば $\omega_r(\zeta)v\neq 0$ だから $\lambda=\mu\circ w_r$ は φ の重みで $\omega_r(\zeta)v\in V_\lambda$ となる．$w_r(h_s)=h_s-n(r,s)h_r$ だから

$$\lambda=\mu\circ w_r=w_r(\mu)$$

が成り立つ．さて $x_r(\zeta)$ を指数関数の定義を用いて展開すれば $\omega_r(\zeta)v$ は

$$\pm\zeta^{i-j+k}\varphi(e_r{}^i/i!)\varphi(e_{-r}{}^j/j!)\varphi(e_r{}^k/k!)v$$

の和となる．そこで ζ について n 次の項をまとめて $\zeta^n v_n$ と表わす．v_n は ζ に無関係で $v\in V_\mu$ だから $v_n\in V_{\mu+nr}$ となる(4.18)．さらに v は $\mathcal{V}_\mu$ の元で $\mathcal{V}$ は許容 $\boldsymbol{Z}$ 形だから $v_n\in\mathcal{V}$ を得る．一方，

$$\omega(\zeta)v=\sum\zeta^n v_n \qquad (v_n\in V_{\mu+nr})$$

の左辺は V_λ の元だから $\lambda\neq\mu+nr$ ならば $v_n=0$ となる(相異なる重みに対する V_μ は一次独立)．したがって上式より $\lambda=\mu+nr$ の時

$$\omega_r(\zeta)v=\zeta^n v_n \qquad (v_n\in\mathcal{V}_\lambda)$$

となる．$\lambda=w_r(\mu)$ だから $n=-\mu(h_r)$．また $v'=v_n$ は ζ に無関係に定まる．すなわち (6.8) が成り立つ． □

(6.9) 随伴表現による Chevalley 群では

$$\omega_r(\zeta)e_s=c(r,s)\zeta^{-n(s,r)}e_{w(s)}$$

が成り立つ．ここで $c(r,s)$ は 1 または -1，$n(s,r)$ は§1 で定義された整数，$w=w_r$ は r に関する対称変換である．$c(r,s)$ は ζ に関係せず r と s だけで定まり次の関係が成り立つ．

$$c(r,s)c(r,-s)=1,\quad c(r,s)c(r,w(s))=(-1)^{n(s,r)}.$$

証明　随伴表現の場合§4で定義した$\mathscr{L}$は許容$\boldsymbol{Z}$形である．随伴表現の重みは根だから $e_s \in \mathscr{L}_s$ に (6.8) を適用すれば

$$\omega_r(\zeta)e_s = c\zeta^{-n(s,r)}e_{w(s)}$$

を得る．ここで $c=c(r,s)$ はζに無関係でrとsとだけで定まる．さらに $ce_{w(s)} \in \mathscr{L}$ だからcは整数である．定義から $\omega_r(\zeta)\omega_r(-\zeta)=1$ が成り立つ．よって $e_s=\omega_r(1)\omega_r(-1)e_s$ より

$$c(r,s)c(r,w(s))=(-1)^{n(s,r)}$$

を得る．ところでcは整数だから $c(r,s)=1$ または -1 である．

$\omega_r(\zeta)$ はLの自己同形だから $[e_s,e_{-s}]=h_s$ の両辺に ω_r を作用させ，(6.6)を用いれば $c(r,s)c(r,-s)=1$ を得る．□

(6.10)　表現φによる一般 Chevalley 群において

$$\omega_r(\zeta)\varphi(e_s)\omega_r(\zeta)^{-1}=c(r,s)\zeta^{-n(s,r)}\varphi(e_{w(s)})$$

が成り立つ．ここで $c(r,s), n(s,r), w(s)$ は (6.9) と同じである．

証明　(6.3) により上式の左辺は $\varphi(\omega_r(\zeta)e_s)$ に等しい．ここでφの中の $\omega_r(\zeta)$ は随伴表現による Chevalley 群の元である．よって (6.9) により上の等式が成り立つ．□

定理 6.11　表現φによる一般 Chevalley 群において次の公式が成り立つ．(記号は (6.9) 参照．さらに $t=w_r(s)$ とおく．)

(1)　$$\omega_r(\zeta)x_s(\eta)\omega_r(\zeta)^{-1}=x_t(c(r,s)\zeta^{-n(s,r)}\eta)$$

(2)　$$h_r(\zeta)x_s(\eta)h_r(\zeta)^{-1}=x_s(\zeta^{n(s,r)}\eta).$$

証明　(6.10)を用いて指数関数を計算すれば(1)の成り立つことがわかる．

(1)および定義6.5により

$$\begin{aligned}h_r(\zeta)x_s(\eta)h_r(\zeta)^{-1}&=\omega_r(\zeta)x_t(c(-1)^{-n(s,r)}\eta)\omega_r(\zeta)^{-1}\\&=x_s(c'\zeta^{-n(t,r)}c(-1)^{-n(s,r)}\eta)\end{aligned}$$

を得る．ここで $c=c(r,s), c'=c(r,w(s))$ だから $c'c=(-1)^{n(s,r)}$ となる((6.9)参照)．$n(t,r)=-n(s,r)$ が成り立つから(2)が証明される．□

4. 対角型の元 $h_r(\zeta)$ の作用　　元 $h_r(\zeta)$ は$\mathscr{V}$上に対角行列のように作用していることを示そう．まず次の補題を証明する．

(6.12)　任意の重みμについて $\mathscr{V}_\mu=\mathscr{V}\cap V_\mu$ とおけば$\mathscr{V}$は$\mathscr{V}_\mu$の直和に分解する．すなわち $\mathscr{V}=\sum\mathscr{V}_\mu$ が成り立つ．

証明 $\{h_r\}$ の基本系の一つを $h_1, \cdots, h_l$ とし，任意の重み μ について $P_\mu = (\mu(h_1), \cdots, \mu(h_l))$ とおく．さらに

$$u = \prod_{i=1}^{l} \binom{h_i - \mu(h_i) + k}{k} \binom{k - h_i + \mu(h_i)}{k}$$

と定義する．h_i の所へ任意の整数値を代入すれば上の右辺は常に整数である．このことから u は §4.6 の記号で h_B と表わされる元の整数係数一次結合となることが容易に証明される．したがって u は包絡環の $\boldsymbol{Z}$ 形 $\mathcal{U}$ の元である．

元 u は $h_1, \cdots, h_l$ の多項式であるが，h_i に $\mu(h_i)$ を代入した時の値は 1 である．しかし λ が μ と異なる重みならば $P_\lambda \neq P_\mu$ で P_λ の各成分は整数となる (4.26)．よって k を十分に大きくとっておけば $u(P_\lambda) = 0$ がすべての重み $\lambda \neq \mu$ について成り立つ．

表現空間 V は部分空間 V_μ の直和に分解する (4.20)．$v \in \mathcal{V}$ に対し

$$v = \sum v_\lambda \qquad (v_\lambda \in V_\lambda)$$

とおけば $uv_\lambda = u(P_\lambda)v_\lambda$ となる．よって

$$uv = \sum uv_\lambda = \sum u(P_\lambda)v_\lambda = v_\mu$$

を得る．$u \in \mathcal{U}$ かつ $\mathcal{V}$ は $\mathcal{U}$ 不変だから $uv = v_\mu \in \mathcal{V} \cap V_\mu = \mathcal{V}_\mu$ が成り立つ．すなわち $\mathcal{V} = \sum \mathcal{V}_\mu$ と直和分解する．▯

(6.13) 任意の r について $h_r(\zeta)$ は $\mathcal{V}_\mu$ の上に

$$h_r(\zeta)v = \zeta^{\mu(h_r)}v \qquad (v \in \mathcal{V}_\mu)$$

と対角型に作用する．

証明 定義により $h_r(\zeta) = \omega_r(\zeta)\omega_r(-1)$ だから (6.8) より上式の成り立つことはほとんど明らかであろう．いま $v \in \mathcal{V}_\mu - \{0\}$ とすれば

$$\omega_r(-1)v = (-1)^{-m}v' \qquad (m = \mu(h_r))$$

をみたす $v' \in \mathcal{V}_\lambda$ がある (6.8)．ここで v' は ζ に関係しないから

$$\omega_r(-\zeta)v = (-\zeta)^{-m}v'$$

も成り立つ．上の 2 式から v' を消去して $\omega_r(-1)v = \zeta^m\omega_r(-\zeta)v$ を得る．この両辺に $\omega_r(\zeta)$ を作用させれば (6.13) が得られる．▯

定理 6.14 表現 φ による一般 Chevalley 群において

$$\omega_r h_s(\zeta)\omega_r^{-1} = h_t(\zeta) \qquad (t = w_r(s))$$

が成り立つ．

証明 (6.12) により $\mathcal{V}=\sum\mathcal{V}_\mu$ が成り立つから，重み μ を定めた時，上式の両辺が $\mathcal{V}_\mu$ 上で同じ作用をしていることを確かめればよい．そこで $\mathcal{V}_\mu$ の元 v をとれば $\omega_r^{-1}v=\omega_r(-1)v$ は $\mathcal{V}_\lambda$ の元である (6.8)．よって (6.13) により

$$\omega_r h_s(\zeta)\omega_r^{-1}v=\omega_r(\zeta^n\omega_r^{-1}v)=\zeta^n v$$

となる．ここで $n=\lambda(h_s)$ であるが $\lambda(h_s)=w_r(\mu)(h_s)=\mu(h_t)$ が成り立つ．したがってすべての $v\in\mathcal{V}_\mu$ について

$$\omega_r h_s(\zeta)\omega_r^{-1}v=h_t(\zeta)v$$

となる．μ は任意だから定理が成り立つ． ∎

§7 一般 Chevalley 群の群造

1. Chevalley の公式 この節では任意の体 F をとりその上で定義された一般 Chevalley 群を G とおく．G を定義する複素半単純 Lie 代数を L，その忠実な表現を φ，表現加群を V とし V に含まれる許容 $\boldsymbol{Z}$ 形を $\mathcal{V}$ とおく．

(6.12)により $\mathcal{V}=\sum\mathcal{V}_\mu$ と直和分解するから各 μ について $\mathcal{V}_\mu$ の基をとりそれらの合併を $\mathcal{V}$ の基とすることができる．このように定めた基を B とおく．§5に従って変数 X を導入し多項式環 $\boldsymbol{Z}[X]$ 上で $x_r(X)$ を $\boldsymbol{Z}[X]\otimes_{\boldsymbol{Z}}\mathcal{V}$ の $\boldsymbol{Z}[X]$ 自己同形として定義する．ここで $t\in F$ を X に代入したものが G の生成元 $x_r(t)$ である．以下

$$X_r=\langle x_r(t)\,|\,t\in F\rangle$$

とおく．(4.23)により $x_r(t_1+t_2)=x_r(t_1)x_r(t_2)$ が成り立つ．まず定理 6.4 が任意の体について成り立つことを証明しよう．

定理 7.1 Δ の元 r,s が一次独立であると仮定する．いま $\{C_{ijrs}\}$ を定理 6.4 で定義された整数の組とすれば

$$x_r(t)x_s(u)x_r(t)^{-1}=x_s(u)\prod x_{ir+js}(C_{ijrs}t^iu^j)$$

が任意の $t,u\in F$ について成り立つ．右辺の積は定理 6.4 と同一である．

証明 $\boldsymbol{Z}$ 上の2変数多項式環を $\boldsymbol{Z}[T,U]$ とすれば $x_r(T),x_s(U)$ が定義され，$\boldsymbol{Z}[T,U]\otimes\mathcal{V}$ の自己同形となる．$\mathcal{V}$ の基 B により行列表示をつくれば行列の各成分は T,U の整数係数多項式となる．これは $x_r(T)^{-1}=x_r(-T)$ についても成り立つ．B の1元 e を定め

$$x_r(T)x_s(U)x_r(T)^{-1}e=\sum P_w(T,U)w \qquad (w\in B)$$

とおけば $P_w(T,U)\in \boldsymbol{Z}[T,U]$ となる．同様に

$$x_s(U)\prod x_{ir+js}(C_{ijrs}T^iU^j)e=\sum Q_w(T,U)w$$

の係数 $Q_w(T,U)$ も $\boldsymbol{Z}[T,U]$ の元である．ところで任意の複素数 ζ,η をとりそれぞれ T,U に代入すれば $x_r(T)$ などが $x_r(\zeta)$ などに移り

$$x_r(\zeta)x_s(\eta)x_r(\zeta)^{-1}e=\sum P_w(\zeta,\eta)w$$

が成り立つ．第2の式についても同様だから定理 6.4 により

$$P_w(\zeta,\eta)=Q_w(\zeta,\eta)$$

がすべての ζ,η について成り立つ．よって多項式として

$$P_w(T,U)=Q_w(T,U)$$

が成り立つ．任意に $t,u\in F$ をとり，それぞれ T,U に代入すれば P_w,Q_w が整数係数の多項式だから $P_w(t,u)$ が F の元として定まり

$$x_r(t)x_s(u)x_r(t)^{-1}e=\sum P_w(t,u)w$$

$$x_s(u)\prod x_{ir+js}(C_{ijrs}t^iu^j)e=\sum Q_w(t,u)w$$

を得る．ところで P_w,Q_w は多項式として一致するから上の両式は同じ元を表わしている．ここで e は B の任意の元で，B は $V_F=F\otimes_Z\mathcal{V}$ の基となるから定理 7.1 が成り立つ． ▯

2. 部分群 U とその構造　　L に対応する根系に基本系 Π を定め，Π によって定まる正系を Δ^+ とおく．その上で

$$U=\langle x_r(t)\mid r\in\Delta^+,t\in F\rangle$$

と定義する．この節では U の構造を調べよう．そのため必要となる補題を証明する．この補題では G は任意の群とする．

(7.2)　G の正規部分群を N とする．さらに H,K は G の部分群でそれぞれ X,Y により生成されていると仮定する．H と K との交換子群 $[H,K]$ を

$$[H,K]=\langle [h,k]\mid h\in H,k\in K\rangle$$

と定義する(『群論』下，第4章§1参照)．任意の $x\in X,y\in Y$ について

$$[x,y]\in N$$

ならば $[H,K]\subset N$ となる．

証明　定義により $[x,y]=xyx^{-1}y^{-1}$ だから $[x,y]\in N$ と

G/N の2元 xN と yN とが交換可能

という条件が同値となる．H の任意の元 h は X の元およびその逆元の積に書

けているから仮定により hN と yN とは可換である．K の元 k は Y の元およびその逆元の積に書けるから hN と kN とは可換で $[h,k]\in N$ を得る．よって定義により $[H,K]\subset N$ が成り立つ． □

基本系 Π を定めれば根の高さ $\mathrm{ht}(r)$ が定義できる．(1.17) により適当な全順序 $>$ が定義され，Δ^+ の元はすべて >0，さらに

$$r\in\Delta, s\in\Delta, r>s \Longrightarrow \mathrm{ht}(r)\geqq\mathrm{ht}(s)$$

が成り立つ．以下このような全順序が定まっていると仮定する．

定理 7.3 任意の正整数 m について

$$U_m=\langle X_r \mid r\in\Delta^+, \mathrm{ht}(r)\geqq m\rangle$$

とおく．この時 $U_1=U\supset U_2\supset\cdots\supset U_h=\{1\}$ は U の中心列である．(『群論』下 p. 418.) U の任意の元は $\prod x_r(t_r)$ $(t_r\in F)$ という形に一意的に書ける．ここで積は r の増加順にとる．任意の体について U はベキ零群である．係数体 F が標数 p の有限体で $|F|=q$ ならば U は p 群で $|U|=q^N$，ここで N は正根の数 $|\Delta^+|$ である．

証明 $r,s\in\Delta^+, \mathrm{ht}(s)\geqq m$ とする．$i>0, j>0$ に対し $ir+js\in\Delta$ ならば，それは正系 Δ^+ の元で $\mathrm{ht}(ir+js)>m$ となる．したがって定理 7.1 から

$$x_r(t)x_s(u)x_r(t)^{-1}\in U_m$$

を得る．すなわち U_m は U の正規部分群である．また定理 7.1 から

$$[x_s(u), x_r(t)]=\prod x_{ir+js}(C_{ijrs}t^i(-u)^j)$$

となる．いま $\mathrm{ht}(s)\geqq m, \mathrm{ht}(r)\geqq n$ とすれば $\mathrm{ht}(ir+js)\geqq m+n$ が成り立つから $[x_s(u), x_r(t)]\in U_{m+n}$ となる．よって (7.2) により

$$[U_m, U_n]\subset U_{m+n}$$

が成り立つ．すなわち $U_1=U\supset\cdots\supset U_h=\{1\}$ は U の中心列である．十分大きく h をとれば $\mathrm{ht}(r)<h$ がすべての r について成り立つから $U_h=\{1\}$ となる．よって U はベキ零群である(『群論』下 p. 420 定理 2.5)．

任意の積 $\prod x_s(t_s)$ を考える．ここで $s\in\Delta^+$，また積の中に同じ根が重複して現われてもよい．しかし隣り合った項が同一の根に属していれば (4.23) を用いて 1 項にまとめる．この積を整理して根の増加順に書きかえることができることを証明しよう．そこで Δ^+ の 1 元 r より小さい根については既に整理ができていて対応する項が左端に寄せられていると仮定する．そこで $s>r$ につい

て逆順に $x_s(u)x_r(t)$ と並んでいるとすれば定理 7.1 より

$$x_s(u)x_r(t)=x_r(t)x_s(u)\prod x_{ir+js}(C_{ijrs}(-t)^i u^j)$$

となる．この右辺に新しく現われる項では $\mathrm{ht}(ir+js)>\mathrm{ht}(r)$ となる．したがって $r<ir+js$ となり r 以下の項は出て来ない．この手段を繰返せば X_r の元をすべて左に移し r まで整理することができる．よって帰納法により U の元は定理 7.3 に述べた形に書けることが証明される．

次にこの表現が一意的であることを証明しよう．そこで

$$y=x_r(t_r)\prod x_s(t_s)$$

において積記号の中に現われる項では $r<s$ が成り立つと仮定する．この時 t_r が y によって一意的に定まることを示せばよい．表現 φ は忠実と仮定したから $\varphi(e_r)\neq 0$, したがって重み λ を適当にとれば $\mathcal{V}_\lambda$ から選んだ基の元 v に対して $\varphi(e_r)v\neq 0$ となる．$v\in\mathcal{V}_\lambda$ だから $\varphi(e_r)v\in\mathcal{V}_{\lambda+r}$ (4.18)．そこで y の右辺の指数関数を展開してみれば

$$yv=v+\varphi(t_r e_r)v+\cdots$$

となる．省略した項は $\mathcal{V}_\mu$ に属する元の F—次結合である．y の表示に現われる根 $r, s, \cdots$ は Δ^+ の元だから省略した項は $\lambda, \lambda+r$ 以外の重みに対応している．異なる重みに対応する $\mathcal{V}_\mu$ の元は一次独立だから t_r は $\mathcal{V}_{\lambda+r}$ に属する元 $\varphi(e_r)v\neq 0$ の係数として一意的に定まる．

係数体 F が標数 p の有限体で $|F|=q$ とすれば q は p のベキである．U の元は上述の形に一意的に書け，t_r は F の任意の元としてよいから U の位数は q^N $(N=|\Delta^+|)$ となる．よって U は p 群である．□

系　すべての $r\in\Delta$ について $t\longmapsto x_r(t)$ は F の加法群から部分群 X_r の上への同形写像である．

証明　定理 1.9(a) により r を含む基本系 Π がある．Π が定める正系に定理 7.3 を適用すれば $x_r(t)=1\Rightarrow t=0$ が成り立つ．対応 $t\longmapsto x_r(t)$ は準同形である (4.23)．それが単射だから系が証明される．□

(7.4)　部分群 U の各元は V_F の線形写像としてベキ単である．適当に V_F の基をとれば U の各元はベキ単上 3 角行列で表現される．

証明　はじめに注意したように $\mathcal{V}$ の基 B は各重み μ に対応する $\mathcal{V}_\mu$ の基を集めたものである．φ の重みの集合には §4.7 で定義した順序が導入されてい

る．そこで B の基を並べる時，その2元 b, b' について

$$b \in \mathcal{V}_\mu, \quad b' \in \mathcal{V}_\lambda, \quad \mu > \lambda$$

ならば b の方が b' より左に並んでいるようにする．この様に基の元を並べた時 $x_r(t)$ の行列表示がどうなっているか調べてみよう．指数関数を展開すれば

$$x_r(t)b = b + t\varphi(e_r)b + t^2\varphi(e_r{}^2/2)b + \cdots$$

となる．ここで $b \in \mathcal{V}_\mu$ とすれば第2項以下は $\mathcal{V}_\lambda$ $(\lambda > \mu)$ の元の一次結合となっている．すなわち b より左に並んでいる基の元の一次結合で書ける．よって $x_r(t)$ を表現する行列はベキ単上3角行列となる．U の生成元はすべてこの様な形をしているから U の各元がベキ単上3角行列で表現される． ▯

(7.5) $\quad r \neq s \Longrightarrow X_r \neq X_s \neq \{1\}, \quad X_r \cap X_s = \{1\}.$

証明 定理7.3系により $X_r \neq \{1\}$ となる．さて r と s とが一次独立ならば定理1.9(b)により r と s を両方とも含む正系 Δ^+ がある．この正系に定理7.3を適用すれば $X_r \cap X_s = \{1\}$ を得る(積表現の一意性)．よって $X_r \neq X_s$ を得る．$s = -r$ の場合は基 B の元を (7.4) の証明のように並べておく．もし $r > 0$ ならば X_r の各元はベキ単上3角行列で表現される．しかし X_{-r} の元はベキ単下3角行列で表現される．したがってこの場合も $X_r \cap X_{-r} = \{1\}$ となる． ▯

3. 部分群 H と N 任意の $r \in \Delta$ と $t \in F^*$ について

$$\omega_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t)$$
$$h_r(t) = \omega_r(t)\omega_r(-1)$$

とおく(定義6.5参照)．さらに $\omega_r = \omega_r(1)$ とおき部分群 N, H を

$$N = \langle \omega_r(t) \mid r \in \Delta, t \in F^* \rangle$$
$$H = \langle h_r(t) \mid r \in \Delta, t \in F^* \rangle$$

と定義する．

(7.6) 次の関係式が成り立つ．($w = w_r$ は r に関する対称変換．)

(i) $\quad \omega_r h_s(t) \omega_r{}^{-1} = h_{w(s)}(t)$

(ii) $\quad \omega_r x_s(t) \omega_r{}^{-1} = x_{w(s)}(c(r,s)t)$

(iii) $\quad h_r(t) x_s(u) h_r(t)^{-1} = x_s(t^{n(s,r)}u)$

ここで $c(r,s), n(s,r)$ は (6.9) と同じである．

証明 変数 T をとり多項式環 $\boldsymbol{Z}[T, T^{-1}]$ を考える．この時 $x_r(T)$ および $x_{-r}(-T^{-1})$ は $\boldsymbol{Z}[T, T^{-1}] \otimes_{\boldsymbol{Z}} \mathcal{V}$ の自己同形となる．さて $\omega_r(T), h_r(T)$ を定

義6.5にならって定義すれば定理7.1の証明と同様の方法により (6.8) および (6.13) に相当する定理が $\omega_r(T), h_r(T)$ について証明される．すなわち

$$v\in\mathcal{V}_\mu \Longrightarrow \omega_r(T)v=T^{-m}v', h_r(T)v=T^m v.$$

ここで $m=\mu(h_r), v'$ は (6.8) で定義された $\mathcal{V}_\lambda$ の元である．したがって任意の体の上で (6.8), (6.13) に当る定理が成り立つ．特に

$$h_r(t)v=t^m v$$

となり $h_r(t)$ は対角行列で表現される．定理6.14と同様に (i) が証明される．(ii), (iii) も対応する定理が複素体の上で成り立つから（定理7.1の証明と同様に）任意の体について証明される． ▯

定理 7.7 Hは可換群で $\langle U, H\rangle$ は U と H との半直積となる．

$$\langle U, H\rangle=UH\triangleright U, \quad U\cap H=\{1\}.$$

またHはNの正規部分群で次の関係が成り立つ．

$$N/H\cong W(\varDelta), \quad N\cap UH=H, \quad N\cap U=\{1\}.$$

証明 基Bに関して各 $h_r(t)$ は対角行列で表現される((7.6)の証明)．したがって $H=\langle h_r(t)\rangle$ は対角行列のつくる群だから可換である．任意の $r, s\in\varDelta$ について(7.6) (iii) から $h_r(t)X_s h_r(t)^{-1}=X_s$ が成り立つ．すなわちHはUの正規化群に含まれている．(7.4)により基の元を適当に並べればUの各元はベキ単上3角行列で表現される．Hの各元は対角行列で表現されるから $U\cap H=\{1\}$ を得る．よって

$$\langle U, H\rangle=UH\triangleright U, \quad U\cap H=\{1\}$$

となり $\langle U, H\rangle$ はUとHとの半直積である．

定義により $\omega_r(t)=h_r(t)\omega_r$ が成り立つから $N=\langle H, \omega_r\ (r\in\varDelta)\rangle$ となる．(7.6) (i) により $\omega_r H\omega_r^{-1}=H$ となるから $H\triangleleft N$ を得る．(7.6) (ii) により $\omega_r X_s\omega_r^{-1}=X_{w(s)}$ $(w=w_r)$ となる．したがってNの各元は部分群の集合 $\{X_s\}$ $(s\in\varDelta)$ に作用している．ところでHの各元はすべての部分群 X_s を不変にするから $W=N/H$ が $\{X_s\}$ に作用する．さて

$$x_r=H\omega_r$$

とおけばWは $\{x_r\ (r\in\varDelta)\}$ で生成される．(7.5)により $\{X_s\}$ と $\varDelta$ とは1対1に対応がついている．そこでX_sとsとを同一視すればx_rは丁度 $W(\varDelta)$ の元w_rと同じ作用を与える．よってWから $W(\varDelta)$ の上への準同形fがあって

$$f(x_r)=w_r \qquad (r\in\Delta)$$

となっている．ここで W の生成集合 $\{x_r\}$ が $x_r{}^2=1, x_r x_s x_r{}^{-1}=x_t$，ここで $t=w_r(s)$，を満足していることを証明しよう．$\omega_r{}^{-1}=\omega_r(-1)$ だから

$$\omega_r{}^{-2}=\omega_r(-1)\omega_r(-1)=h_r(-1)\in H.$$

したがって $x_r{}^2=1$ を得る．また $\omega_s(1)=x_s(1)x_{-s}(-1)x_s(1)$ より

$$\omega_r\omega_s\omega_r{}^{-1}=x_t(c)x_{-t}(-c')x_t(c)$$

を得る((7.6)(ii))．ここで $t=w_r(s)$ とおいた．(6.9) により

$$c=\pm 1, \quad cc'=c(r,s)c(r,-s)=1$$

だから定義により $\omega_r\omega_s\omega_r{}^{-1}=\omega_t(c)=h_t(c)\omega_t$，すなわち

$$x_r x_s x_r{}^{-1}=x_t \qquad (t\in w_r(s))$$

が成り立つ．したがって定理 1.15(b) により $W(\Delta)$ から W の上への準同形 g があって $g(w_r)=x_r$ $(r\in\Delta)$ となる．明らかに fg, gf はそれぞれ $W(\Delta), W$ の恒等写像であるから W は $W(\Delta)$ と同形となる．

最後の関係式 $N\cap UH=H$ を証明するために次の補題が必要である．

(7.8)　N の元 n に対応する $W(\Delta)$ の元を w とする．すなわち上の記号で

$$f(Hn)=w$$

とする．この時，任意の $s\in\Delta$ について $nX_sn^{-1}=X_{w(s)}$ が成り立つ．

証明　N の生成集合 $\{\omega_r(t)\}$ の各元について $\omega_r(t)$ に対応する $W(\Delta)$ の元は $w=w_r$ であって $\omega_r(t)X_s\omega_r(t)^{-1}=X_{w(s)}$ が成り立つ．f は同形写像だから (7.8) が成り立つ．▯

定理 7.7 の証明にもどる．(7.4) の証明のように基の元を並べれば UH の元は上 3 角行列で表現される．一方，ω_r は $\mathcal{V}_\mu$ の基を $\mathcal{V}_\lambda$ $(\lambda=w_r(\mu))$ の中に動かしている((7.6)の証明参照)．さて N の元 n に対応する $W(\Delta)$ の元を w とおけば，n を表現する行列は $F\otimes\mathcal{V}_\mu\to F\otimes\mathcal{V}_{w(\mu)}$ をみたす．そこで n が UH の元であるとすれば，n に対応する $W(\Delta)$ の元 w はすべての重み μ について $w(\mu)=\mu$ をみたす．ところで忠実な表現 φ について (4.26) が成り立つ．すなわち $\Gamma_\varphi\supset P$ となる．よって w がすべての重みを不変にすれば，w はすべての根を不変にする．したがって $w=1$ となり $n\in H$ を得る．よって

$$UH\cap N\subset H$$

が成り立つ．逆の包含関係は自明だから $UH\cap N=H$ となる．さて

$$N\cap U\subset N\cap UH\cap U=H\cap U=\{1\}$$

だから $N\cap U=\{1\}$ が証明される． □

4. Chevalley 群の Tits 系　以下 $B=UH$ とおき (B,N) が BN 対をつくることを証明しよう．一般に群 G の部分群 B,N が与えられ

(T1)　$G=\langle B,N\rangle, H=B\cap N\lhd N,$

(T2)　$W=N/H$ は位数2の元からなる集合 S により生成される，

(T3)　任意の $s\in S, w\in W$ に対して

$$wBs\subset BwB\cup BwsB,$$

(T4)　任意の $s\in S$ について $sBs\neq B$,

という4条件をみたしている時 (G,B,N,S) は **Tits 系**をつくるという． B と N とを特に取り上げて (B,N) 対ともいう(『群論』上 p.317)．さて $w\in W$ とすれば条件 (T1) により w を代表する元 $n\in N$ をどの様にとっても剰余類 Bn, nB は一定のものになる．そこで

$$Bn=Bw,\quad nB=wB$$

などの記法を用いる．($nH=Hn$ だが $nB=Bn$ とは限らない．)

以下 $G=G(\Delta)$ は Δ 型の一般 Chevalley 群，Π を一つの基本系とし，Π が定める正系を Δ^+ とおく．$U=\langle X_r\,|\,r\in\Delta^+\rangle$，さらに $r\in\Delta^+$ について

$$U_r=\langle X_s\,|\,s\in\Delta^+-\{r\}\rangle$$

とおく．まず補題を三つ証明しよう．

(7.9)　(i)　$U=X_rU_r=U_rX_r\rhd U_r$ が成り立つ．

(ii)　さらに $r\in\Pi$ ならば $\omega_rU_r\omega_r^{-1}=U_r$ となる．

証明　(i)　$s\in\Delta^+-\{r\}$ ならば $i\geqq 0, j>0$ の時 $ir+js\in\Delta^+-\{r\}$ となる．よって定理7.1により $U_r\lhd U$ を得る．明らかに $U=\langle X_r, U_r\rangle$ だから (i) が成り立つ．

(ii)　$s\in\Delta^+-\{r\}$, $r\in\Pi$ ならば $w_r(s)\in\Delta^+-\{r\}$ が成り立つ (1.10)．したがって (7.6) (ii) により (ii) が成り立つ． □

(7.10)　$r\in\Delta^+$ ならば $X_{-r}\subset\{1\}\cup X_rH\omega_rX_r$ が成り立つ．

証明　$\omega_r(t)$ の定義から $t\neq 0$ ならば

$$x_{-r}(-t^{-1})=x_r(-t)\omega_r(t)x_r(-t)\in X_rH\omega_rX_r$$

が成り立つ． □

(7.11) $r\in\Pi$ ならば $B\cup B\omega_r B$ は部分群となる．すなわち

$$\omega_r B\omega_r\subset B\cup B\omega_r B.$$

証明 $G_0=B\cup B\omega_r B$ とおく．$x\in G_0$ ならば $x^{-1}\in G_0$ となる．これは $\omega_r^{-1}=h_r(-1)\omega_r$ から直ちに証明される． よって G_0 が部分群となるための条件は (7.11) にあげた包含関係が成り立つことである．さて

$$\omega_r B\omega_r=\omega_r(X_r U_r H)\omega_r^{-1}=\omega_r X_r\omega_r^{-1}(\omega_r U_r H\omega_r^{-1})$$

となる．したがって (7.6) および (7.9) (ii) より

$$\omega_r B\omega_r=X_{-r}U_r H\subset B\cup B\omega_r B$$

を得る．最後の包含関係は (7.10) による． □

定理 7.12 $G(\Delta)$ は (B,N) 対をもつ．いま $S=\{H\omega_r\ (r\in\Pi)\}$ とおけば (G,B,N,S) は Tits 系をつくる．

証明 (7.10) により $r\in\Delta^+$ ならば $X_{-r}\subset\langle B,N\rangle$，したがって

$$G=\langle B,N\rangle$$

となる． 定理 7.7 により $B\cap N=H\lhd N$ となる． また $N/H=W$ は根系の Weyl 群 $W(\Delta)$ と同形だから W は S により生成されている(定理 1.12)． すなわち条件 (T1), (T2) が成り立つ．

いま N から任意の元 n をとり，n に対応する $W(\Delta)$の元を w とおく．(7.8) により $nX_r n^{-1}=X_{w(r)}$ が成り立つ．さて $r\in\Pi$ と仮定すれば

$$nB\omega_r=nX_r U_r H\omega_r=X_{w(r)}n\omega_r U_r H$$

を得る((7.9) (ii) および (7.6))．そこで $w(r)\in\Delta^+$ と仮定すれば

$$nB\omega_r\subset Bn\omega_r B$$

となるからこの場合 (T3) が成り立つ．つぎに $w(r)\notin\Delta^+$ とすれば

$$w\omega_r(r)=w(-r)=-w(r)\in\Delta^+$$

となる．したがって n の代りに $n\omega_r$ をとれば

$$n\omega_r B\omega_r\subset Bn\omega_r\omega_r B=BnB$$

が成り立つ．よって $Bn\omega_r B\omega_r B=BnB$ を得る．さて

$$\begin{aligned} nB\omega_r &\subset Bn\omega_r B\omega_r B\omega_r \\ &\subset Bn\omega_r B\cup Bn\omega_r B\omega_r B \end{aligned}$$

((7.11) を用いた) が成り立つ．最後の項は BnB に等しいからこの場合にも (T3) が成り立つ．

$r\in\Pi$ ならば $\omega_r B\omega_r=\omega_r B\omega_r^{-1}\supset X_{-r}$ だから (T4) も成り立ち定理が証明される. ▯

5. Tits 系をもつ群 この節では Tits 系(G, B, N, S)をもつ群Gについて一般に成り立つ2, 3の定理を証明する. 記号も前節で用いたものを続けて用いることにする. 群 $W=N/H$ をGの **Weyl 群**という. 一般の場合 Wは根系に対応するとは限らないが Coxeter 群となることが知られている (『群論』上 p. 334).

条件 (T3) の両辺の逆元をとり記号を書き替えれば

(T3)′ $$sBw\subset BwB\cup BswB \qquad (s\in S, w\in W)$$

の成り立つことがわかる. 帰納法により $s_i\in S$ ならば

(7.13) $$(Bs_1\cdots s_nB)(BwB)\subset\bigcup Bs_i\cdots s_kwB$$

を得る. ここで右辺は $i<\cdots<k$ をみたす $\{1, \cdots, n\}$ の部分集合すべてについて和集合をとるのである. そこでSの任意の部分集合Jをとり

$$W_J=\langle J\rangle, \quad P_J=BW_JB$$

(ここで BW_JB は BwB $(w\in W_J)$ の和集合)とおけば (7.13) より P_J はGの部分群となる. 特に

(7.14) $$G=BWB=\{BwB\ (w\in W)\}$$

が成り立つ. ここで $BwB=Bw'B\Leftrightarrow w=w'$ が成り立つことを証明しよう. そのため $w\in W$ の長さ $l(w)$ を

$$l(w)=\min\{l\,|\,w=s_1s_2\cdots s_l\ \ (s_i\in S)\}$$

と定義する. $l(w)=0$ ならば $w=1$ である.

(7.15) $$BwB=Bw'B\Longleftrightarrow w=w'.$$

証明 $l=l(w)\leqq l(w')$ と仮定し l に関する帰納法による. $l=0$ の時は w' が $B\cap N=H$ の元で代表されるから $w'=1$ となり (7.15) が成り立つ. そこで $l>0$ と仮定し $w=w''s, l(w'')=l-1$ と表わす. この時

$$Bw=Bw''s\subset Bw'B$$

より $Bw''\subset Bw'Bs\subset Bw'B\cup Bw'sB$ を得る(T3). 帰納法の仮定により $w''=w'$ または $w''=w's$ となる. ところで $l(w')\geqq l$ だから第1の等式は成り立たない. したがって $w'=w''s=w$ を得る. ▯

(7.16) $w\in W, s\in S$ に対し次の命題が成り立つ.

(i) $l(sw)\geqq l(w) \Longrightarrow sBw\subset BswB$.

(ii) $l(sw)\leqq l(w) \Longrightarrow sBw\cap BwB\neq\emptyset$.

証明 (i) $l=l(w)$ とおき l に関する帰納法による．$l=0$ ならば (i) は自明である．そこで $l>0$ とし $w=w'r, l(w')=l-1$ と表わす．この時 $l(sw')\geqq l-1$ となる．よって帰納法の仮定を用いて

$$sBw=sBw'r\subset Bsw'Br\subset Bsw'B\cup BswB$$

を得る．一方，(T3)′ により $sBw\subset BwB\cup BswB$ が成り立つ．ところで $Bsw'B$ と BwB に共通元があれば $Bsw'B=BwB$ となる．よって前補題 (7.15) により $sw'=w$ を得る．すなわち $w'=sw$ となり $l(sw)\geqq l$ という仮定に矛盾する．したがって $Bsw'B$ と BwB に共通な元はない．すなわち sBw の元はすべて $BswB$ の元となり (i) が成り立つ．

(ii) (T3) と (T4) により $B\neq sBs\subset B\cup BsB$ を得る．したがって

$$sBsw\cap BsBw\neq\emptyset$$

が成り立つ．$w'=sw$ に (i) が適用できるから $sBsw\subset BwB$ となる．よって $sBw\cap BwB\neq\emptyset$ を得る．▯

(7.17) W の元 w を S の元の積として表わした時 w の最短表示を

$$w=s_1s_2\cdots s_l \qquad (s_i\in S, l=l(w))$$

とすれば，すべての i について次式が成り立つ．

$$Bs_iB\subset\langle B, wBw^{-1}\rangle.$$

証明 l に関する帰納法による．$l(s_1w)<l(w)$ だから (7.16) を用い

$$s_1Bw\cap BwB\neq\emptyset$$

すなわち $s_1B\subset BwBw^{-1}B\subset\langle B, wBw^{-1}\rangle$ を得る．そこで

$$w_1=s_1w$$

とおけば帰納法の仮定により $Bs_iB\subset\langle B, w_1Bw_1{}^{-1}\rangle$ $(i=2, 3, \cdots, l)$ が成り立つ．ところで $s_1B\subset\langle B, wBw^{-1}\rangle$ だから

$$\langle B, w_1Bw_1{}^{-1}\rangle\subset\langle B, wBw^{-1}\rangle$$

となり $Bs_iB\subset\langle B, wBw^{-1}\rangle$ $(i\geqq 1)$ が成り立つ．▯

(7.18) S の真の部分集合 J で W を生成することはできない．

証明 $\langle J\rangle=W$ と仮定して矛盾を導こう．J に含まれていない S の元を r とする．仮定により (G, B, N, J) は Tits 系をつくる．r を J の元の積とし

て表わした時の最短表示を $r=s_1\cdots s_n$ $(s_i\in J)$ とおき，Jを生成集合としたTits 系 (G,B,N,J) に (7.17) を適用すれば

$$Bs_iB\subset\langle B,rBr\rangle$$

を得る．一方 Tits 系 (G,B,N,S) の条件 (T3) より

$$\langle B,rBr\rangle\subset B\cup BrB$$

となる．よって $Bs_iB=B$ または $Bs_iB=BrB$ を得るから (7.15) により

$$s_i=1 \quad \text{または} \quad s_i=r$$

となり矛盾が得られる．したがって $\langle J\rangle\neq W$ である． ▯

定理 7.19 (G,B,N,S) を Tits 系とする．

(i) G の部分群 P が B を含んでいれば S の部分集合 J が定まり

$$P=P_J=BW_JB$$

となる．また $P_J=P_K\Rightarrow J=K$.

(ii) S の部分集合 J,K に対して $P_J\cap P_K=P_{J\cap K}$ が成り立つ．同様に

$$W_J\cap W_K=W_{J\cap K}.$$

(iii) $P_J\supset gBg^{-1}\Rightarrow g\in P_J$.

(iv) $N_G(P_J)=P_J$.

(v) P_J と P_K が G の中で共役ならば $J=K$ となる．

(vi) G の中心を $Z(G)$ とおけば $Z(G)\subset B$ が成り立つ．

証明 (i) $P\supset B$ とすれば P は B に関する両側剰余類の和集合である．そこで $BwB\subset P$ と仮定し，w を S の元の積として表わした時の最短表示の一つを $w=s_1\cdots s_n$ とおく．(7.17) により

$$Bs_iB\subset\langle B,wBw^{-1}\rangle\subset P$$

を得る．そこで

$$J=\{s\mid s\in S, BsB\subset P\}$$

とおけば $BwB\subset P\Leftrightarrow w\in\langle J\rangle$ が成り立つ．すなわち $P=P_J$ となる． さて S の部分集合をとり $P=P_K$ と仮定する．定義から明らかに $K\subset J$ が成り立つ．もし $K\neq J$ ならば K に含まれていない J の元 r をとる．この時 $BrB\subset P_K=BW_KB$ だから (7.15) により r は K の元の積として表わされる．これは W が $S-\{r\}$ で生成できることを示しているから (7.18) に矛盾する．したがって $K=J$ となり (i) が証明される．

(ii) (i) により $P_J\cap P_K=P_I$ をみたす部分集合 I がある．ところで

$$I=\{s\mid s\in S, BsB\subset P_J\cap P_K\}$$

だから $I=J\cap K$ となる．$W_J\cap W_K$ についても同様である．

(iii) $G=BWB$ だから $g\in BwB$ をみたす $w\in W$ がある．この時

$$\langle B, gBg^{-1}\rangle=\langle B, wBw^{-1}\rangle$$

が成り立つ．(7.17) により $BwB\subset\langle B, wBw^{-1}\rangle$ を得るから

$$g\in BwB\subset\langle B, gBg^{-1}\rangle\subset P_J$$

を得る．(iv), (v), (vi) は (iii) の系である． ▯

6. Chevalley 群の元の標準形 定理 7.12 により一般 Chevalley 群は Tits 系をもつからその元は bnb' $(b, b'\in B, n\in N)$ と書くことができる．この表わし方は一意的でないが元 b, b' を適当に制限して一意的な表示が得られる．これを元 x の**標準形**という．以下，元の標準形について述べよう．

まず U と同様に部分群 V を

$$V=\langle x_{-r}(t)\mid r\in\Delta^+, t\in F\rangle$$

と定義する．(7.6) (iii) により VH は部分群となり $VH\triangleright V$ が成り立つ．また (7.4) と同様に基の元を並べれば V の各元はベキ単下 3 角行列で表現される．したがって

$$UH\cap VH=H,\quad UH\cap V=\{1\} \tag{7.20}$$

が成り立つ．

一般 Chevalley 群では $N/H\cong W(\Delta)$ だから $w\in W$ に対して (7.8) の様に

$$f(Hn)=w$$

をみたす N の元 n を一つ定める．この時，任意の $r\in\Delta$ について

$$nX_rn^{-1}=X_{w(r)}$$

が成り立つ (7.8)．さて

$$U_w^+=U\cap n^{-1}Un,\quad U_w^-=U\cap n^{-1}Vn$$

とおく．H の元による共役写像は U も V も不変にするから w に対応する代表元 n の選び方によらず U_w^+, U_w^- は w だけにより定められる部分群である．ところで (7.20) により $U\cap V=\{1\}$ だから

$$U_w^+\cap U_w^-=\{1\}$$

となる．(7.8) を用いれば容易にわかるように

$$r\in\varDelta^+,\ w(r)\in\varDelta^+ \Longrightarrow X_r\in U_w^+$$

$$r\in\varDelta^+,\ w(r)\in-\varDelta^+ \Longrightarrow X_r\in U_w^-$$

が成り立つ．したがって $U=\langle U_w^+, U_w^-\rangle$ となるが実は $U=U_w^+U_w^-$ が成り立つことを証明しよう．一般に次の命題が成り立つ．

(7.21)　根の集合 $\varDelta$ に任意の全順序を与えておく．この時 U の元は与えられた順序に従ってつくる積 $\prod x_r(t_r)$ の形に一意的に書ける．

証明　$\varDelta$ に与えた順序が $r<s \Rightarrow \mathrm{ht}(r)\leqq\mathrm{ht}(s)$ をみたしている場合は定理 7.3 において証明されている．そこでこの順序 T_0 を一つ定め U の元 x を $x=x_1x_2\cdots x_h$ と表わす．ここで各 i について x_i は $\mathrm{ht}(r)=i$ をみたす根 r に関する $x_r(t_r)$ を順序 T_0 に従ってかけた積である．定理 7.3 により x はこの様な形に一意的に書くことができる．さて部分群 U_m を定理 7.3 のように定義すれば

$$U_1\supset U_2\supset\cdots\supset U_h=\{1\}$$

は U の中心列である．さて (7.21) で $\varDelta$ に与えられた順序を T とおく．ここで任意の m に対し

$$x=\prod x_r(t_r)y_my_{m+1}\cdots y_h \tag{7.22}$$

(ここで最初の積は $\mathrm{ht}(r)<m$ をみたす根 r について $x_r(t_r)$ を順序 T に従ってつくった積で，各 y_i は $\mathrm{ht}(s)=i$ をみたす根 s について $x_s(t_s)$ を順序 T_0 に従ってかけ合わせた積) という形に一意的に書けることを証明しよう．

$m=1$ の場合は定理 7.3 により成り立つから m に関する帰納法を用いる．そこで (7.22) が成り立つと仮定し，$y_m=\prod x_s(t_s)$ とおく．次の段階に移るために各 $x_s(t_s)$ を順序 T に従って指定した場所に動かさねばならない．これは適当な交換子を加えれば可能である．ところで $\{U_i\}$ が中心列だから追加した交換子はすべて U_{m+1} に含まれている．したがって x は

$$x=\prod x_r(u_r)z_{m+1}\cdots z_h \tag{7.23}$$

と書け，最初の積は $\mathrm{ht}(r)<m+1$ をみたす根すべてについて順序 T に従った積となり z_i は $h(s)=i$ をみたす根に関する積となる．この様な表現の一意性は次のように証明される．(7.23) のはじめの積において $\mathrm{ht}(s)$ が丁度 m となる項を右に動かし，順序 T_0 に従って並べれば (7.22) の表示が得られる．これは U_{m+1} に含まれる交換子をつけ加えれば可能である．したがって (7.23)

においてFの元 u_r は一意的に定まる．残りの $z_{m+1}, \cdots, z_h$ の一意性は定理 7.3から得られる．

$m=h+1$ の場合が (7.21) であるから命題が成り立つ． □

(7.24) 任意の $w\in W$ について $U=U_w^+U_w^-$ が成り立つ．

証明 $w(r)\in -\varDelta^+$ をみたす正根が $w(s)\in\varDelta^+$ をみたす正根より後になるように順序をつければ (7.21) より $U=U_w^+U_w^-$ となる． □

定理 7.25 一般 Chevalley 群 G の Weyl 群を W とおく．任意の $x\in G$ に対して $x\in BwB$ をみたす w が一意的に定まる．しかも

$$x=unv \qquad (u\in U, n\in N, v\in U_w^-)$$

と書け (u,n,v) は x により一意的に定まる．

証明 (7.14) および (7.15) により $x\in BwB$ をみたす $w\in W$ が一意的に定まる．さて w に対応する N の元 n をとれば $nU_w^+n^{-1}\subset U$ だから

$$BwB=BnHU_w^+U_w^-=BnU_w^-=UHnU_w^-$$

となる．よって適当に $n\in N$ を選べば $x=unv$ $(u\in U, v\in U_w^-)$ という形に書ける．一意性を証明するために

$$unv=ymz \qquad (y\in U, m\in N, f(Hm)=w, z\in U_m^-)$$

とおけば，$m=hn$ $(h\in H)$ と書ける．したがって

$$n(vz^{-1})n^{-1}=u^{-1}yh\in nU_w^-n^{-1}\cap UH$$

が成り立つ．ところで $nU_w^-n^{-1}\subset V$ だから (7.20) により

$$vz^{-1}=1, \qquad u^{-1}yh=1$$

を得る．すなわち $v=z$ および $h=y^{-1}u\in H\cap U=\{1\}$ が成り立つ．したがって $u=y, n=m, v=z$ となり x の表示は一意的に定まる． □

BnB に含まれている B の剰余類は Bnv $(v\in U_w^-)$ という形に一意的に書ける(定理 7.25)．したがって G が有限体上で定義されていれば両側剰余類 BnB は丁度 $|U_w^-|$ 個の左剰余類の和集合である．よって B の指数は

$$\sum|U_w^-|$$

に等しい．U_w^- の元は $\prod x_r(t_r)$ $(r\in\varDelta^+, w(r)\in -\varDelta^+)$ という形に一意的に表わすことができる(7.21)．よって次の結果を得る．

(7.26) G が有限体上で定義されている場合 $|F|=q$ とおけば

$$|G:B|=\sum q^{n(w)}=\sum q^{l(w)}$$

が成り立つ(定理1.13参照).

7. 部分群 U の正規化群　定理7.7により $U \lhd B$ であるが次の定理が成り立つ.

定理 7.27　B は U の正規化群 $N_G(U)$ と一致する.

証明　$N_G(U)$ は B を含む部分群だから定理7.19により $N_G(U)=P_J$ となる S の部分集合 J がある. ところで J の元 s をとれば s は少なくとも一つの正根 r の符号を変える. したがって $sX_rs^{-1}=X_{s(r)}\subset V$ となる. 一方,

$$sX_rs^{-1}\subset sUs^{-1}=U$$

が成り立つから $sX_rs^{-1}\subset U\cap V=\{1\}$ という矛盾がおこる. よって J は空集合で $N_G(U)=B$ となる. □

§8 普遍 Chevalley 群

1. 部分群 H の構造　前節と同様に G は任意の体 F 上で定義された一般 Chevalley 群とする. G を定める複素半単純 Lie 代数を L, その忠実な表現を φ とおく. この時 φ の表現空間 V の許容 $\boldsymbol{Z}$ 形 $\mathcal{V}$ があって G は

$$V_F=F\otimes_{\boldsymbol{Z}}\mathcal{V}$$

の可逆 F 線形写像のつくる群である(§4.8). さて (6.12) により

$$\mathcal{V}=\sum\mathcal{V}_\mu$$

と φ の重み μ に対応する部分空間 $\mathcal{V}_\mu$ の直和に分解する. よって

$$V_F=\sum(V_F)_\mu, \quad (V_F)_\mu=F\otimes_{\boldsymbol{Z}}\mathcal{V}_\mu$$

となる. 部分群 H を調べるに当って基本となるのは次の命題である.

(8.1)　H の元 $h_r(t)$ は V_F に対角型に作用する. すなわち

$$v\in(V_F)_\mu \Longrightarrow h_r(t)v=t^{n(\mu,r)}v$$

が成り立つ. ここで $n(\mu,r)=\mu(h_r)$ でそれは整数である.

証明　$v\in\mathcal{V}_\mu$ の時, 上式が成り立つことは (7.6) の証明中において述べた. よって上式が任意の $v\in(V_F)_\mu$ について成り立つ. t の指数が整数であることは (4.26) において証明されている. □

定理 8.2　任意の $r\in\Delta$ について $h_r(t_1)h_r(t_2)=h_r(t_1t_2)$ が成り立つ. 部分群 H は可換群で $\{h_r(t)\,|\,r\in\Pi\}$ により生成される.

証明　任意の $v\in(V_F)_\mu$ について

$$h_r(t_1)h_r(t_2)v=(t_1t_2)^{n(\mu,r)}v$$

となる．したがって $h_r(t_1)h_r(t_2)=h_r(t_1t_2)$ が成り立つ．

Hの各元は対角型に作用するからHは可換群である．その生成集合を求めよう．さて $\{h_r\}$ は根系であって(2.1)，$\varDelta$ の基本系 $\varPi$ を定めれば

$$\{h_p\ (p\in\varPi)\}$$

が $\{h_r\}$ の基本系となる．そこで $\varPi=\{r_1,\cdots,r_l\}$ とおき r_i に対応するHの元を h_i と書くことにすれば $\{h_1,\cdots,h_l\}$ が基本系となる．よって

$$h_r=a_1h_1+\cdots+a_lh_l \qquad (a_i\in\boldsymbol{Z})$$

と表わすことができる．いま μ を重みとすれば

$$n(\mu,r)=\mu(h_r)=\sum a_i\mu(h_i)$$

が成り立つ．そこで $v\in(V_F)_\mu$ をとれば

$$h_r(t)v=(\prod h_i(t)^{a_i})v$$

を得る．よって任意の $r\in\varDelta$ に対する $h_r(t)$ が $\{h_i(t)\}$ のベキ積で表わされる．すなわちHは $\{h_i(t)\}$ で生成されている． □

定理 8.3 前定理の証明において定義されたHの生成集合を $\{h_i(t)\}$ とする．この時 $\prod h_i(t_i)=1$ となるための条件は任意の重み μ について

$$\prod t_i^{n(\mu,r_i)}=1$$

が成り立つことである．Hの構造は重み格子 $\varGamma_V$ によって定まる．

証明 $v\in(V_F)_\mu$ とすれば $\prod h_i(t_i)=x$ の作用は

$$xv=\prod t_i^{n(\mu,r_i)}v$$

である(8.1)．よって定理の前半が成り立つ．

定理における条件は μ について線形であるから，すべての重み μ について条件が成り立っていれば重みの生成する格子 $\varGamma_V$ の各元について条件が成り立つ．すなわちHの構造は生成元の間に成り立つ関係によって定まるから，Hは $\varGamma_V$ により定まる． □

(8.4) もし $\varGamma_V=Q$ ならば (§4.9参照)，Hの元は

$$\prod h_i(t_i) \qquad (t_i\in F^*)$$

と一意的に書ける．したがってHはFの乗法群 F^* の l 個の直積と同形である．

証明 定理 8.2 の証明において示したように

$$h_r(t)=\prod h_i(t)^{a_i}=\prod h_i(t^{a_i})$$

が成り立つから H の元は $\prod h_i(t_i)$ $(t_i\in F^{\#})$ と書ける．その表わし方が一意的であることを証明するには

$$\prod h_i(t_i)=1 \Longrightarrow t_1=\cdots=t_l=1$$

を示せばよい．そこで $\prod h_i(t_i)=1$ と仮定する．定理 8.3 により

$$\prod t_i^{n(\mu,r_i)}=1$$

がすべての $\mu\in\Gamma_V$ について成り立つ．仮定により $\Gamma_V=Q$ だから §4.9 の記号を用いて $q_1,q_2,\cdots,q_l\in\Gamma_V$ となる．さて $\mu=q_i$ ならば

$$n(\mu,r_j)=\delta_{ij}$$

すなわち $i=j$ の時 $q_i(r_j)=1$，$i\neq j$ の時 $q_i(r_j)=0$ となる．よって

$$\text{すべての } \mu\in Q \text{ について } \prod t_i^{n(\mu,r_i)}=1 \Longrightarrow t_i=1$$

が成り立つ．したがって H の元は $\prod h_i(t_i)$ と一意的に表わされる． □

2. 普遍 Chevalley 群　この節では半単純複素 Lie 代数 L を一つ定める．その上で L の忠実な表現 φ をいろいろとり，φ による一般 Chevalley 群の間の関係を調べよう．φ の重みの生成する格子を Γ_φ とおく．(4.26)により

$$Q\supset\Gamma_\varphi\supset P$$

が成り立つ．ここで Q は $\mathscr{H}$ の双対格子，P は L の根が生成する加法群である(§4.9 参照)．

定義 8.5　$\Gamma_\varphi=Q$ の時 φ による一般 Chevalley 群を**普遍的**であるという．このことを $G=G^u$ と表わす．また $\Gamma_\varphi=P$ の時 G は**随伴的**であるという．G が随伴的である時 $G=G^a$ と書き，G を（随伴を省略して）単に Chevalley 群という．

定理 8.6　任意の体 F の上で表現 φ による一般 Chevalley 群を G とする．同じ体の上で同じ Lie 代数からつくられた普遍 Chevalley 群を G^u とおく．この時 G^u から G の上への準同形 $f=f_\varphi$ があって $\ker f$ は G^u の中心に含まれる．すなわち $G^u/\ker f\cong G$ となり G^u は G の中心拡大である．

証明　Lie 代数 L に対応する根系を Δ とする．任意の根 r と F の任意の元 t に対して記号 $x'_r(t)$ を定め $\{x'_r(t)\}$ から生成され次の諸関係により定義される群を G' とおく．関係は

(A) $$x'_r(t_1)x'_r(t_2)=x'_r(t_1+t_2) \qquad (r\in\Delta)$$

(B) $$x'_r(t)x'_s(u)x'_r(t)^{-1}=x'_s(u)\prod x'_{ir+js}(C_{ijrs}t^iu^j)$$

ここで $s\neq\pm r$，積の順序および C_{ijrs} は定理 7.1 と同一とする.

また $\omega'_r(t), h'_r(t)$ を定義 6.5 にならって定義すれば

(C) $h'_r(t)$ と $h'_s(u)$ は可換で (7.6) の関係式が成り立つ.

さらに任意の $r\in\Delta$ について

(D) $$h'_r(t)h'_r(u)=h'_r(tu)$$

が成り立つ. 一般 Chevalley 群 G の生成元の集合 $\{x_r(t)\}$ がこれらの関係をみたしていることはそれぞれ (4.23)，定理 7.1，定理 7.7，(7.6) および定理 8.2 において示されている. よって生成元とその間の関係によって定義された群の定義により (『群論』上 p.165 参照)

$$x'_r(t)\longmapsto x_r(t)$$

は G' から G の上への準同形 θ に拡張される.

上に定義した群 G' が普遍 Chevalley 群 G^u と同形であることを証明しよう. 根系 Δ の中に基本系 Π を定め，それによって定まる正系を Δ^+ とおく.

$$U'=\langle x'_r(t)\,|\,r\in\Delta^+\rangle$$

とおけば θ は U' から G の部分群 U の上への準同形写像を引きおこす. 定理 7.3 の証明の第 2 段階をくり返せば U' の元は $\prod x'_r(t_r)$ という形に書けることが証明される. この元の θ による像は $\prod x_r(t_r)$ で，U において表現は一意的だから (定理 7.3) U' について表現の一意性が証明される. すなわち θ は U' から U の上への同形写像を引きおこしている.

群 G' の中に $N'=\langle\omega'_r(t)\,|\,r\in\Delta\rangle$，$H'=\langle h'_r(t)\,|\,r\in\Delta\rangle$ および

$$V'=\langle x'_r(t)\,|\,r\in-\Delta^+\rangle$$

を定義する. $\theta(V')$ は §7.6 で定義した部分群 V と一致する. よって

$$\theta(U'\cap V'H')\subset\theta(U')\cap\theta(V'H')=U\cap VH=\{1\}$$

を得る (7.20). θ は U' の上で同形写像だから $U'\cap V'=\{1\}$ となる. よって (7.5) も G' について成り立つ. 定理 7.12 の証明がそのまま G' にあてはまるので G' は Tits 系をもっている. そこで G' の元 x は

$$x=u'n'v'\qquad(u'\in U', n'\in N', v'\in(U')^-_w)$$

と表わすことができる. この時 $w\in W$ は x により一意的に定まる.

さて $\ker\theta=K$ とおいて $K\subset H'\cap Z(G')$ となることを証明しよう. そこ

で K の元 x をとり $x=u'n'v'$ と上の様に分解する．$x\in K$ だから

$$1=\theta(u')\theta(n')\theta(v')$$

となる．ここで θ が N'/H' から N/H の上への同形写像を引きおこしていることに注意すれば $\theta(n')$ に対応する W の元はやはり w である．G の中での標準形の一意性（定理 7.25）により $w=1, \theta(u')=\theta(v')=1$ を得る．このことから $n'\in H'$, $u'=v'=1$ を得るから $x\in H'$ が証明される．すなわち $K\subset H'$ が成り立つ．この時

$$[U', K]\subset U'\cap K\subset U'\cap H'=\{1\}$$

となる．（関係（7.6）により H' は U' を正規化する．）同様に

$$[V', K]=\{1\}$$

も成り立つ．よって K は G' の生成集合の各元と可換だから K は G' の中心 $Z(G')$ に含まれる．すなわち $K\subset H'\cap Z(G')$ が成り立つ．

基本系 Π の元を $r_1, r_2, \cdots, r_l$ とし r_i に対応する H' の生成元を $h_i'(t)$ と表わす．ここで H' の元が $\prod h_i'(t_i)$ $(t_i\in F^*)$ と書けることを証明しよう．そのように書くことのできる元全体のつくる集合を H'' とおく．H' は可換群で (D) をみたすから H'' は H' の部分群となる．そこで H' の生成元 $h_r'(t)$ がすべて H'' の元であることを証明すれば $H'=H''$ となる．もし $r\in\Pi$ ならば当然 $h_r'(t)\in H''$ が成り立つ．一般の場合には定理 1.12 により $r=w(r_i)$ をみたす $r_i\in\Pi$ と $w\in W$ とがある．$l(w)$ に関する帰納法を用いる．そこで $w=w_s w'$ $(l(w')=l(w)-1, s\in\Pi)$, $a=w'(r_i)$ とおけば帰納法の仮定により $h_a'(t)$ は H'' の元である．ここで

$$h_a'(t)\omega_s'(u)h_a'(t)^{-1}=\omega_{\prime}^{s}(t^{n(a,s)}u)$$

が成り立つことに注意する（関係式（7.6）と ω' の定義）．さて

$$\begin{aligned} h_r'(t)&=h'_{w_s(a)}(t)=\omega_s' h_a'(t)(\omega_s')^{-1}\\ &=\omega_s'\omega_s'(t^{n(a,s)})^{-1}h_a'(t)\\ &=h_s'(t^{n(a,s)})_a'^{-1}h(t)\in H'' \end{aligned}$$

（第3の等号は（7.3）(i)）となる．よって $H''=H'$ が成り立つ．すなわち H' の任意の元は $\prod h_i'(t_i)$ と書けている．

ここで $G=G^u$ が普遍的と仮定する．さて $x=\prod h_i'(t_i)$ の θ による像は $\theta(x)=\prod h_i(t_i)$ となるから（8.4）により $t_1, t_2, \cdots, t_l$ が一意的に定まる．よって $x\in$

$\ker\theta \Rightarrow t_1=\cdots=t_l=1 \Rightarrow x=1$, すなわち準同形写像 θ は実は同形写像である.

上述のように G^u と G' が同形で, G' から G の上への準同形写像があるから, これらの写像の合成を f とおけば f は G^u から G の上への準同形でその核は G^u の中心に含まれている. □

(8.7) Δ 型普遍 Chevalley 群を G とおく. 任意の $r\in\Delta$ について

$$\langle x_r(t), x_{-r}(s)\rangle \qquad (t, s\in F)$$

は $SL(2,F)$ と同形である.

証明 $G_r=\langle x_r(t), x_{-r}(s)\rangle$ とおく. 定理 1.9(a) により $r\in\Pi$ と仮定することができる. G_r の生成元の集合は A_1 型普遍 Chevalley 群の生成関係をみたしている. さて A_1 型普遍 Chevalley 群は $SL(2,F)$ と同形である (§5.2 参照, 自然表現の重みは q_1 と $-q_1$ である). よって

$$SL(2,F) \longrightarrow G_r$$

という準同形がある (定理 8.6). もしこの準同形が単射でなければ G_r の中で $h_r(t)=1$ という関係が成り立つ. ところが $G_r\subset G$ で G は普遍的だから $h_r(t)=1 \Longrightarrow t=1$ となり上の準同形が単射でないという仮定に矛盾する. すなわち $SL(2,F)\cong G_r$ が成り立つ. □

注意 1. L を A_l 型複素単純 Lie 代数とすれば L は自然に $l+1$ 次元空間 V に作用している. この自然表現による一般 Chevalley 群が普遍的であることを証明しよう. L の中で対角行列の全体が Cartan 部分代数となる. よって $h_r=e_{ii}-e_{jj}$, 特に基本系は

$$h_1=e_{00}-e_{11}, \quad h_2=e_{11}-e_{22}, \quad \cdots, \quad h_l=e_{l-1,l-1}-e_{ll}$$

である. 表現空間 V に自然な基 $e_0, e_1, \cdots, e_l$ をとれば

$$(\sum\lambda_i e_{ii})e_k=\lambda_k e_k$$

だから $\mu_k : \sum\lambda_i e_{ii} \longmapsto \lambda_k$ は自然表現の重みである. (4.24) で定義した Q の元 $\{q_i\}$ をとれば

$$\mu_0=q_1, \quad \mu_1=q_2-q_1, \quad \cdots, \quad \mu_{l-1}=q_l-q_{l-1}, \quad \mu_l=-q_l$$

となる. したがってこの場合 $\Gamma_V=Q$ となり普遍的な Chevalley 群が得られる. この場合 $\mu_0=q_1$ が最高の重みである.

L が C_l 型の場合も同様で自然表現による一般 Chevalley 群は普遍的である. しかし L が B_l 型の場合, 自然表現の重みは根の一部で $\Gamma_V=P$ となる. また D_l 型の場合, 根の集合は §3.4 の記号で $\{\pm e_i\pm e_j\}$ である. 自然表現の重みの集合は $\{\pm e_i\}$ となる. この場合は

$$h_1=e_{11}-e_{22}-e_{l+1,l+1}+e_{l+2,l+2}$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$h_{l-1}=e_{l-1,l-1}-e_{ll}-e_{2l-1,2l-1}+e_{2l,2l}$$

$$h_l=e_{l-1,l-1}+e_{ll}-e_{2l-1,2l-1}-e_{2l,2l}$$

だから $e_1=q_1, e_2=q_2-q_1, \cdots, e_{l-2}=q_{l-2}-q_{l-3}$ だが

$$e_{l-1}=q_l+q_{l-1}-q_{l-2}, \quad e_l=q_l-q_{l-1}$$

となる．したがって

$$Q \supsetneqq \Gamma_V \supsetneqq P$$

となっている．$\Gamma_V \neq P$ でも表現空間 V 上の一般 Chevalley 群が随伴的な群と必ずしも違っているわけではない．第5章最後の注意参照.

注意 2. 定理 8.6 の証明から次の定理の成り立つことがわかる.

定理 8.6′ 生成元の集合 $\{x_r'(t)\}$ $(r\in\Delta, t\in F)$ と関係 (A), (B), (C), (D) により定義される群は体 F 上の Δ 型普遍 Chevalley 群である.

実際，Δ の次元が $\geqq 2$ の場合，関係 (C) は (A), (B), (D) から導かれる関係で特に取り上げる必要はないことが知られている (Steinberg [6] 参照). ▯

3. f_φ の核 表現 φ による一般 Chevalley 群の構造は定理 8.6 において定義された準同形 f_φ の核によって定まる．この節ではその核の構造を調べよう．部分群 H の元は

$$x=\prod h_i(t_i) \qquad (t_i\in F^\#)$$

と表わすことができる(定理 8.2)．任意の重み μ に対して

$$\prod t_i^{\mu(h_i)}$$

は $F^\#$ の元であるが，この値は x だけによって定まる．すなわち

$$\prod h_i(t_i)=\prod h_i(s_i)$$

とすれば $\prod h_i(t_i(s_i)^{-1})=1$ となる．よって定理 8.3 により

$$\prod (t_i s_i^{-1})^{\mu(h_i)}=1$$

が成り立つ．すなわち

$$\chi_x : \mu \longmapsto \prod t_i^{\mu(h_i)}$$

と定義される関数 χ_x が重みの生成する格子 Γ_V の上で定まる．この形から明らかなように χ_x は格子 Γ_V から $F^\#$ の中への指標である．すなわち

$$\chi_x(\mu+\mu')=\chi_x(\mu)\chi_x(\mu'), \quad \chi_x(0)=1$$

が成り立つ．Γ_V から $F^\#$ の中への指標（略して F 指標という）の全体は

$$\chi\chi'(\mu)=\chi(\mu)\chi'(\mu)$$

と定義される積により群をつくる．この群は $\mathrm{Hom}(\Gamma_V, F^\#)$ と表わされる.

(8.8) 表現 φ による一般 Chevalley 群を G，φ の重みの生成する格子を

Γ_V とおく．Γ_V の F 指標 χ が χ_x $(x\in H)$ となるための条件は χ が重み加群 Q（定義 4.25）の F 指標に拡張できることである．Q の F 指標に拡張できる Γ_V の F 指標の全体を H' とおけば

$$x \longmapsto \chi_x$$

は H から H' の上への同形写像である．

証明 いま $\chi_x : \mu \longmapsto \prod t_i^{\mu(h_i)}$ とする．任意の $q\in Q$ について，q が h_i でとる値 $q(h_i)$ は整数だから $\prod t_i^{q(h_i)}$ が F^* の元として確定する．明らかに $q \longmapsto \prod t_i^{q(h_i)}$ は Q の F 指標で χ_x の拡張となっている．

逆に F 指標 χ が Q の F 指標に拡張できると仮定する．その拡張も χ と表わし $t_i=\chi(q_i)$ とおく．ここで $\{q_i\}$ は $\{h_i\}$ の双対基である．Q の任意の元は $\{q_i\}$ の整数係数一次結合となるから任意の $\mu\in\Gamma_V$ は

$$\mu=\sum n_i q_i \qquad (n_i\in \boldsymbol{Z})$$

と表わすことができる．$\{q_i\}$ が $\{h_i\}$ の双対基だから $n_i=\mu(h_i)$ となる．よって

$$\chi(\mu)=\prod \chi(q_i)^{n_i}=\prod t_i^{\mu(h_i)}$$

となる．そこで $x=\prod h_i(t_i)$ とおけば $x\in H$ かつ $\chi=\chi_x$ が成り立つ．

上に定義した集合 H' は明らかに $\mathrm{Hom}(\Gamma_V, F^*)$ の部分群である．任意の元 $x, y\in H$ について $\chi_x\chi_y(\mu)=\chi_{xy}(\mu)$ が成り立つから $x \longmapsto \chi_x$ は H から H' の上への準同形である．定理 8.3 によりこの写像は単射となり命題が証明される．▯

普遍 Chevalley 群 G^u において H に対応する群を H^u と表わす．表現 φ による一般 Chevalley 群を G とおき定理 8.6 で定義された準同形を f_φ とする．定理 8.6 の証明から f_φ の核は $H^u\to H$ の核と一致することがわかる．

(8.9) 次の図式は可換である．

$$\begin{array}{cccc} f_\varphi : & H^u & \longrightarrow & H \\ & \downarrow & & \downarrow \\ & \mathrm{Hom}(Q, F^*) & \longrightarrow & H' \subset \mathrm{Hom}(\Gamma_V, F^*) \end{array}$$

ここで縦矢は (8.8) の写像 $x \longmapsto \chi_x$，下の横矢は重み加群 Q から Γ_V への制限写像である．

証明 (8.4) により H^u の元は $\prod h_i(t_i)$ と一意的に表わすことができる．こ

の時，定義により対応する指標 χ は

$$q_j \longmapsto \prod t_i^{q_j(h_i)} = t_j$$

となる．よって χ の Γ_V 上への制限は (8.8) の証明中で計算したように

$$\mu \longmapsto \prod t_i^{\mu(h_i)}$$

をみたす．これは $x=\prod h_i(t_i)\in H$ に対応する指標 χ_x である．

定理 8.6 の証明から H^u の元 $\prod h_i(t_i)$ の f_φ による像が x と一致することがわかる．よって図式 (8.9) は可換である．□

定理 8.10　f_φ の核は $\mathrm{Hom}(Q/\Gamma_V, F^*)$ と同形である．

証明　自然な埋め込み写像 $\Gamma_V\to Q$ から完全系列

$$0 \longrightarrow \Gamma_V \longrightarrow Q \longrightarrow Q/\Gamma_V \longrightarrow 0$$

が得られる．そこで Hom 関手の一般的性質により(『代数』 II, p. 295 定理 2)

$$1 \longrightarrow \mathrm{Hom}(Q/\Gamma_V, F^*) \longrightarrow \mathrm{Hom}(Q, F^*) \longrightarrow \mathrm{Hom}(\Gamma_V, F^*)$$

が完全系列となる．(8.9) の可換図式とあわせて

$$\ker f_\varphi \cong \mathrm{Hom}(Q/\Gamma_V, F^*)$$

を得る(『代数』 II, p. 337 補題 2)．□

注意　忠実な表現 φ_1, φ_2 が与えられた時 φ_i の重みが生成する格子を Γ_i とおく．もし $\Gamma_1\subset\Gamma_2$ ならば φ_2 による Chevalley 群 G_2 から φ_1 による一般 Chevalley 群 G_1 の上への準同形 g があって $\ker g$ は $\mathrm{Hom}(\Gamma_2/\Gamma_1, F^*)$ と同形になる．□

4. Q/P の構造　　重み加群を Q, 根が生成する加群を P とおく．P も Q も階数 l の自由加法群であるから Q/P は有限群であって，その構造は P の基を Q の基の一次結合で表わした時の係数がつくる行列の単因子によって定まる(『代数』 II, pp. 278—282)．前のように P の基 $\{r_1, \cdots, r_l\}$ をとる．$\mathcal{H}$ の基として $\{h_1, \cdots, h_l\}$ をとれば行列

$$C=(a_{ij}),\quad a_{ij}=r_i(h_j)$$

は§2 で定義した根系 Δ の Cartan 行列と一致する．

(8.11)　重み加群 Q に $\{h_i\}$ の双対基 $\{q_1, \cdots, q_l\}$ をとり各 r_i を

$$r_i=\sum c_{ij}q_j$$

と $\{q_j\}$ の一次結合として表わす．この時，行列 (c_{ij}) は Δ の Cartan 行列と一致する．

証明　定義により $q_k(h_j)=0\ (k\neq j), q_k(h_k)=1$ となる．よって

$$r_i(h_j)=\sum c_{ik}q_k(h_j)=c_{ij}$$

が成り立つ．すなわち行列 (c_{ij}) は Δ の Cartan 行列と一致する． □

定理 8.12 D_l 型の場合を除けば Q/P は巡回群でその位数は次の表で与えられる．

A_l	B_l	C_l	G_2	F_4	E_6	E_7	E_8
$l+1$	2	2	1	1	3	2	1

l が奇数ならば D_l 型でも Q/P は位数 4 の巡回群であるが，l が偶数の場合 D_l 型では Q/P は位数 2 の巡回群二つの直積である．

証明 §3 において各型の根系はすべて書き上げられているからそれを用いれば Cartan 行列 C は容易に求められる．その上で C の単因子を計算すればよい．各根系について別々に実行してみよう．

A_l 型　この場合 C は対角線上に 2 が並び，それに沿って上下に -1 があるだけでその他の成分は 0 である．単因子を求めるには行列式の値が 1 の整数成分をもつ行列を右，左からかけて C を対角行列に直せばよい（『代数』 II，p. 278）．そこで

$$(I+e_{21})\text{ 右},\quad (I-e_{21}+e_{31})\text{ 左},\quad (I+e_{12})\text{ 右}$$

とかければ最初の単因子 1 が現われ，次に一つ次数の下った行列で第 1 列が

$${}^t(3,-2,0,\cdots,0)$$

その他は C と同一のものが得られる．第 2 の単因子も 1 で，同様の手段を繰り返せば最後に

$$\begin{pmatrix} l & -1 \\ -(l-1) & 2 \end{pmatrix}$$

が現われる．結局，単因子は $1,1,\cdots,1,l+1$ であることがわかる．したがって Q/P は位数 $l+1$ の巡回群である（『代数』 I，p. 99 定理 2）．

B_l 型　Cartan 行列は最後の列を除けば A_l 型の Cartan 行列と一致するが最後の列は ${}^t(0,\cdots,0,-2,2)$ となる．したがって単因子の計算の最後に

$$\begin{pmatrix} l & -2 \\ -(l-1) & 2 \end{pmatrix}$$

が現われるから単因子は $1,1,\cdots,1,2$ となる．よってこの場合 Q/P は位数 2 の巡回群である．

C_l 型 Cartan 行列は B_l 型のものの転置行列である．したがって単因子は前の場合と一致する．

D_l 型 この場合も Cartan 行列は最後の行と列とを除けば A_l 型のものと一致する．最後の行と列では -1 が $l-2$ 番目の成分となっている．したがって最後から2番目に

$$\begin{pmatrix} l-1 & -1 & -1 \\ -(l-2) & 2 & 0 \\ -(l-2) & 0 & 2 \end{pmatrix}$$

を得る．よって最後には

$$\begin{pmatrix} 2 & 0 \\ l-2 & 2 \end{pmatrix}$$

の単因子を計算すればよい．l が奇数ならば単因子は $\{1,4\}$，l が偶数ならば $\{2,2\}$ である．したがってこの場合も定理が成り立つ（『代数』 I，p.99 定理2）．

G_2 型 $(r_1, r_1)<(r_2, r_2)$ とすれば Cartan 行列は

$$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

で行列式の値は1となる．したがって単因子は $\{1,1\}$ である．

E_6 型 §3.7の記号を用いる．Cartan 行列は対角線上に2が並ぶ対称行列で (i, j) 成分 $(i<j)$ は

$$(i,j)=(1,3),(2,4),(3,4),(4,5),(5,6)$$

の場合 -1 でその他の場所は0となる．これから単因子は 1,1,1,1,1,3 であることがわかる．

その他の例外型の場合も§3にあげた根系から容易に Cartan 行列が求まる．その単因子を計算すれば定理の成り立つことが確かめられる． ▯

注意 Cartan 行列など根系の性質や不変量に関したことは Bourbaki [1] の巻末にまとめてあるから参照されたい． ▯

5. 有限 Chevalley 群の位数

定理 8.13 有限体 F 上の普遍 Chevalley 群を G とする．対応する根系を Δ，その基本系の一つを Π，Π の定める正系を Δ^+，Weyl 群を W とおく．

$$|F|=q, \qquad |\Pi|=l, \qquad |\Delta^+|=N$$

とすれば G の位数は次式で与えられる.

$$|G|=q^N(q-1)^l\sum q^{l(w)}$$

ここで和は $w\in W$ のすべてにわたり, $l(w)$ は w の最短表示の長さである.

証明 (7.26) により B の指数は $\sum q^{n(w)}$ に等しい. ここで $n(w)$ は w により符号を変える正根の数である. ところで定理 1.13 により $n(w)=l(w)$ が成り立つ. 定理 7.7 により $B=UH, U\cap H=\{1\}$ であるから

$$|B|=|U|\cdot|H|$$

となる. 定理 7.3 により $|U|=q^N$, (8.4) により $|H|=(q-1)^l$ を得る. □

有限体上で随伴的な Chevalley 群の位数を求めるには次の定理を証明すればよい.

定理 8.14 F は有限 q 元体とする. Q/P の位数を e とし, さらに

$$d=|\mathrm{Hom}(Q/P, F^*)|$$

とおく (§8.4 参照). Q/P が巡回群の場合には

$$d=(e, q-1) \qquad (e \text{ と } q-1 \text{ との最大公約数})$$

となる. D_l 型で l が偶数の場合には F の標数が 2 ならば $d=1$, F の標数が 2 でなければ $d=4$ となる.

証明 Q/P が巡回群の場合にはその生成元を x とおく. Q/P から F^* の中への準同形 f は $f(x)\in F^*$ により定まる. F^* は位数 $q-1$ の巡回群だから(『代数』 I, p. 102 例 4) $d=(e,q-1)$ となる. D_l 型で l が偶数の場合には Q/P は位数 2 の巡回群二つの直積である(定理 8.12). したがって F の標数が 2 の場合 F^* の位数に奇数だから $d=1$ となる. その他の場合は $d=4$ である. □

定理 8.15 係数体 F が標数 p の有限体とする. F 上の一般 Chevalley 群を G とおけば部分群 U, V は G のシロー p 群である.

証明 仮定により q は p のベキであるから U は位数 q^N の p 群である. 明らかに $l(w)=0$ は w が 1 の時にだけ成り立つ. したがって

$$|G:B|=\sum q^{l(w)}\equiv 1 \pmod{p}$$

が成り立つ. また H の位数は $(q-1)^l$ の約数だから p と素である. よって部分群 U の指数が p と素になるから U は G のシロー p 群である. V は U と同位数だから V も G のシロー p 群となる. □

注意 1. 定理8.13が与えるGの位数は実際に$|G|$を計算しようとすると不便なものである．古典型の Chevalley 群の位数は第2章で求めたが，それと比較すると全く異質のものであることがわかる．実は古典型の場合と同様に

$$|G|=(1/d)q^N(q^{d(1)}-1)\cdots(q^{d(l)}-1)$$

という形の公式が成り立つ．ここで$d(1),\cdots,d(l)$は根系Δにより定められる正整数である．この結果については Chevalley の原論文 [2*] に Lie 群論を用いる位相的な証明があり，また Solomon による代数的な証明が Steinberg [6], Carter [2] にのっているから参照されたい．例外型の場合の $d(1),\cdots,d(l)$ を表にしておこう．

G_2型	2, 6
F_4型	2, 6, 8, 12
E_6型	2, 5, 6, 8, 9, 12
E_7型	2, 6, 8, 10, 12, 14, 18
E_8型	2, 8, 12, 14, 18, 20, 24, 30

注意 2. 定理8.14の証明から Q/P が巡回群ならば $\mathrm{Hom}(Q/P, F^*)$ も巡回群であることがわかる．Chevalley 群における部分群Hの構造も容易に書き上げることができる．Q/P が巡回群の時は

$$H\cong(F^*)^{l-1}\times C$$

でCは位数 $(q-1)/d$ の巡回群である．D_l型でlが偶数の場合にはqが奇数ならばHは $(F^*)^{l-2}\times D^2$ でDは位数 $(q-1)/2$ の巡回群である．▯

§9 Chevalley 群の単純性

この節では単純複素 Lie 代数に対応する随伴的 Chevalley 群 $G(\Delta)$ が四つの例外を除けば単純群になることを証明する．基本となるのは次の Tits の補題である．

(9.1) Tits 系 (G, B, N, S) をもつ群 Gが次の4条件をみたすと仮定すればGは単純群である．

(1) Gは交換子群G'と一致する．

(2) Bは可解群である．

(3) Gの正規部分群でBに含まれているものは $\{1\}$ だけである．

(4) Sは既約，すなわちSの部分集合JについてJの各元と $S-J$ の各元とが交換可能であればJはSと一致するかまたはJは空集合である．

証明 Gの正規部分群をG_0とする．G_0が正規だからBG_0はGの部分群でBを含んでいる．よって定理7.19により $BG_0=BW_JB$ をみたすSの部分集

合 J がある．この時 $r\in J$ と $s\in S-J$ とが交換可能であることを証明しよう．明らかに $l(rs)>l(s)$ だから (7.16) により $rBs\subset BrsB$ を得る．$r\in J$ だから $G_0\cap BrB$ は空集合ではない．$G_0\lhd G$ より

$$G_0\cap sBrBs\neq\emptyset$$

となる $(s=s^{-1})$．ところで $sBrBs\subset sBrsB$ だから (T3) により

$$sBrBs\subset BrsB\cup BsrsB$$

を得る．したがって G_0 は $BrsB$ または $BsrsB$ の元を含んでいる．もし G_0 が $BrsB$ の元を含めば $BG_0\supset BrsB$ より $rs\in W_J$ を得る．$r\in J$ と仮定したから $s\in W_J$ となり (7.18) に矛盾する．したがって G_0 は $BsrsB$ の元を含んでいる．上と同様に $srs\in W_J$ を得る．この場合 $K=\{r,s\}$ とおけば $srs\in W_J\cap W_K$ となる．ところで $W_J\cap W_K=W_{J\cap K}=\langle r\rangle$ となる(定理 7.19(ii))．すなわち $srs=r$，$sr=rs$ が成り立つ．条件 (4) により S は既約だから $J=S$ または J は空集合となる．

いま $J=S$ ならば $BG_0=BWB=G$ となる．したがって同形定理により

$$G/G_0\cong B/B\cap G_0$$

が成り立つ．この右辺は条件(2)により可解群である．さて $\overline{G}=G/G_0$ とおけば条件 (1) により $\overline{G}$ は交換子群と一致する．一方，$\overline{G}$ は可解だから $\overline{G}$ は $\{1\}$ と一致する．すなわち $G=G_0$ となる．

最後に J が空集合と仮定する．この場合は $BG_0=B$，すなわち $G_0\subset B$ となる．よって条件(3)により $G_0=\{1\}$ を得る．この様に G の正規部分群 G_0 は G に一致するかまたは $\{1\}$ となる．よって G は単純群である． □

Chevalley 群の単純性を証明するために次の補題が入用となる．

(9.2) 部分群 V は U と共役になる．すなわち $w_0\in W(\Delta)$ が

$$w_0(\Delta^+)=-\Delta^+$$

をみたしていれば ((1.14)(b) 参照) $w_0Uw_0^{-1}=V$ となる．

証明 $r\in\Delta^+$ ならば $s=w_0(r)\in-\Delta^+$ となる．そこで w_0 の任意の代表元 $n\in N$ をとれば $nX_rn^{-1}=X_s$ $(s=w_0(r))$ をみたす(7.8)．明らかにこれから $nUn^{-1}=V$ が得られる． □

以上の準備の下で Chevalley 群の単純性が証明される．

定理 9.3 係数体 F 上の Δ 型(随伴的) Chevalley 群を G とおく．次にあ

げる四つの例外を除けば G は単純群である．例外は

$$|F|=2, \Delta=A_1, B_2, G_2 \text{ および } |F|=3, \Delta=A_1.$$

証明　定理 7.12 により G は Tits 系 (G, B, N, S) をもっている．以下 G が (9.1) の条件をみたすことを証明しよう．まず

$$B=UH \triangleright U, \quad B/U \cong H$$

で H は可換群（定理 7.7），U はベキ零群（定理 7.3）だから B は可解群で条件 (2) が成り立つ．

条件 (3) を証明するために B に含まれている正規部分群を K とおく．この時 $wUw^{-1}=V$ をみたす N の元 w があるから (9.2)，

$$K \subset B \cap wBw^{-1} = UH \cap VH = H$$

となる (7.20)．定理 8.6 の証明と同様の方法を用い K が G の中心に含まれることが証明される．一方，H の元 y に対応する指標を $\chi=\chi_y$ とおけば

$$(9.4) \qquad yx_s(u)y^{-1}=x_s(\chi(s)u)$$

を得る（(7.6) (iii)）．よって $y \in K$ ならば $y \in Z(G)$ だから $\chi(s)=1$ がすべての根 s について成り立つ．ところで G は随伴的だから（重みと根とが一致し）定理 8.3 により $y=1$ を得る．すなわち $K=\{1\}$ で条件 (3) が成り立つ．

Δ 型の Chevalley 群では Dynkin の図形が連結だから S は既約である．すなわち条件 (4) が成り立つ．

最後に条件 (1) が例外の場合を除けば成り立つことを証明しよう．まず係数体 F が $|F| \geqq 4$ をみたすと仮定する．(7.6) (iii) により

$$h_r(t)x_r(u)h_r(t)^{-1}=x_r(t^2u)$$

が成り立つ．したがって $[h_r(t), x_r(u)]=x_r((t^2-1)u)$ を得る．$|F| \geqq 4$ だから $t^2 \neq 0, 1$ をみたす F の元 t がある．ゆえに任意の r と u とについて $x_r(u)$ は交換子となる．すなわち G は交換子で生成されるから $G=G'$ が成り立つ．よってこの場合，条件 (1) が成り立つ．

以下 $|F| \leqq 3$ と仮定する．例外の場合は除くから $\Delta \neq A_1$ と仮定する．Δ の任意の元 r に対し $w(r) \in \Pi$ をみたす $w \in W(\Delta)$ がある（定理 1.12）．この時 X_r と $X_{w(r)}$ とは共役だから (7.8)，

$$r \in \Pi \Longrightarrow X_r \subset G'$$

を証明の目標とする．さて Π の Dynkin の図形の中に r と丁度 1 重に結ばれ

ている根 s があると仮定する．この時 r と s とは A_2 型の根系を生成するから s の r 系列は $\{s, r+s\}$ となる．したがって定理 7.1 により

$$[x_s(u), x_r(t)] = x_{r+s}(\varepsilon tu) \qquad (\varepsilon = \pm 1)$$

を得る．すなわち $x_{r+s}(t)$ は任意の t について交換子となる．ところで

$$w_s(r+s) = r$$

が成り立つから $x_r(t) \in G'$ を得る．§2 で述べた Lie 代数の分類定理により $\varDelta = A_l$ $(l \geqq 2), D_l, E_l, F_4$ の場合，すべての $r \in \Pi$ について上の条件をみたす根 s が存在するから $\varDelta$ 型の群について条件 (1) が成り立つ．

さて $l>2$ ならば $\varDelta = B_l$ で r が長い根の場合，$\varDelta = C_l$ で r が短い根の場合にはやはり $X_r \subset G'$ となる．このいずれかの場合 r を短い根とし，r が s と 2 重に結ばれていれば s の r 系列は $\{s, s+r, s+2r\}$ となり

$$[x_s(u), x_r(t)] = x_{s+r}(\varepsilon ut) x_{s+2r}(\varepsilon' t^2 u)$$

が成り立つ．ここで $\varepsilon, \varepsilon'$ は 1 または -1 である．$r+s$ は短い根で $s+2r$ は長い根だから X_{r+s} か X_{s+2r} のいずれかは G' に含まれている．よって上式より両方とも交換子群に含まれている．すなわち $\varDelta$ が B_l でも，C_l でも $l>2$ ならば条件 (1) が成り立つ．

$\varDelta = B_2$ の場合，上の様に r, s を選び交換子を計算すれば

$$[x_{s+r}(u), x_r(t)] = x_{2r+s}(ctu)$$

となり $c = \pm 2$ である．よって $|F| = 3$ ならば $X_{2r+s} \subset G'$ となる．$l>2$ の場合と同様に $X_{r+s} \subset G'$ を得るからこの場合も条件 (1) が成り立つ．

$\varDelta = G_2$ の場合 r を短い根，s を長い根とし s の r 系列を

$$\{s, s+r, s+2r, s+3r\}$$

とおく．正の根はこの外に r と $2s+3r$ がある．交換子の計算により

$$[x_s(u), x_{s+3r}(t)] = x_{2s+3r}(\varepsilon tu) \qquad (\varepsilon = \pm 1)$$

を得る．よって長い根に対応する X は G' に含まれる．また

$$[x_{r+s}(u), x_r(t)] = x_{2r+s}(c_1 tu) x_{3r+2s}(c_2 tu^2) x_{3r+s}(c_3 t^2 u)$$

ここで $c_1 = \pm 2$ である．$2r+s$ は短い根で，右辺に現われる他の根は長い根であるから，$|F| = 3$ ならば短い根に対応する群も G' に含まれる．□

注意 1. 定理 9.3 の証明の要点は例外の場合を除けば各生成元 $x_r(t)$ が交換子群の元となることの証明である．これは一般 Chevalley 群の場合にもそのままあてはまる．す

なわち例外の場合を除けば一般 Chevalley 群は (9.1) の条件(1)をみたしている．例外の場合 Chevalley 群 G は $G' \neq G$ をみたすことを示そう．A_1 型の場合はすでに（II §2）述べたから B_2 型と G_2 型の場合を調べる．いずれの場合も係数体は2元体で，G は普遍的である．

B_2 型　各生成元 $x_r(1)$ を -1 にうつす写像が G から乗法群 $\{\pm 1\}$ の上への準同形に拡張されることを証明しよう．そのためには G の基本関係（定理 8.6 参照）において各 $x_r(1)$ に -1 を代入した式が成り立つことを確かめればよい．（A）において t_1, t_2, t_1+t_2 のうち0でない項の数は偶数だから，この場合はよい．（B）において，積記号の中は $x_{r+s}(1)x_{2r+s}(1)$ または $x_{r+s}(2)$ となる．$|F|=2$ だから後者は1となり（B）も成り立つ．定義から

$$\omega_r \longmapsto -1, \quad h_r(t) \longmapsto 1$$

となるから（C),（D）共に成り立ち $x_r(1) \longmapsto -1$ は基本関係を保つ写像となる．よってそれは G から $\{\pm 1\}$ の上への準同形に拡張される．すなわち G は指数2の正規部分群を含むから $G' \neq G$ である．実際2元体上の B_2 型の群は6次の対称群 Σ_6 と同形である．

G_2 型　この場合 r が長い根の時 $x_r(1)$ を1に，r が短い根の時 $x_r(1)$ を -1 に対応させれば G から $\{\pm 1\}$ の上への準同形が得られる．関係 (A),(C),(D) を保つことはすぐわかる．（B）における積記号の中に短い根が現われるのは定理 6.4 の最後の三つの場合のいずれかである．しかしその第1の場合，短い根に対応する元は $N_{r,s}=\pm 2$ より消えてしまう．その他の場合，短い根に対応する項が二つ現われるからやはり関係（B）が成り立つ．よって B_2 型の場合と同様に G と交換子群 G' とは一致しない．この場合，指数2の正規部分群はユニタリ群 $SU(3,3)$ と同形であることが知られている．

注意 2. 例外の場合も含めて，普遍 Chevalley 群 G^u から随伴 Chevalley 群 G^a への準同形の核は G^u の中心 $Z(G^u)$ と一致する．また，この注意と定理 8.6 から Δ 型の Chevalley 群は Δ と F だけで定まり Lie 代数 L の標準基の取り方などには関係しないことがわかる．▯

§10　Steinberg 群

1. 定義　前節において単純複素 Lie 代数に対応する Chevalley 群がほとんどすべての場合，単純群であることを証明した．そこで有限体上の古典群の大部分と，例外型 Chevalley 群が有限単純群となることがわかった．ユニタリ群は Chevalley 群ではないが A_l 型の群の自己同形を適当にとると，その自己同形の不変元のつくる部分群としてユニタリ群が現われる．この事実をもとにして，残りの有限古典群の外に2種類の単純群を Steinberg が構成した．これらの群を Steinberg 群という．

この構成のもととなるのはグラフ型自己同形の概念である．A_l, D_l, E_6 型の根系に対応する Dynkin の図形は恒等写像でない自己同形 σ をもっている．たとえば A_l 型では中央の点に関する対称写像である．

(10.1) Δ を A_l, D_l または E_6 型の根系とし，恒等写像でない図形の自己同形を σ とおく．複素数体上の Δ 型単純 Lie 代数を L, Δ の基本系の一つを Π とおく．Π に属する根が生成する Euclid 空間を E とおけば，σ は E の等長写像 τ に拡張される．この等長写像 τ により Δ は不変である．任意の体 F 上の Δ 型普遍 Chevalley 群を G とおけば G は

$$\gamma(x_r(t)) = x_{\tau(r)}(\varepsilon_r t)$$

をみたす自己同形 γ をもつ．ここで $\varepsilon_r = \varepsilon_{-r}$ で $\varepsilon_r = 1$ または -1 である．

証明 Δ の根はすべて同一の長さをもつので，その長さを 1 に定める．この時 Π の 2 根 r, s に対応する Dynkin の図形の白丸が線分で結ばれているかいないかに応じて (r, s) は $-1/2$ または 0 となる．したがって

$$(r, s) = (\sigma r, \sigma s) \qquad (r, s \in \Pi)$$

が成り立つ．基本系 Π は E の基だから σ は一意的に E の等長写像 τ に拡張できる．任意の $r \in \Delta$ に関する対称変換を w_r とおけば

$$\tau w_r \tau^{-1} = w_{\tau(r)}$$

が成り立つ．いま $r \in \Pi$ と仮定すれば $\tau(r) = \sigma(r) \in \Pi$ だから τ による共役写像は Δ の Weyl 群 W の生成集合 $\{w_r\}$ $(r \in \Pi)$ を不変にする．したがって $\tau W \tau^{-1} = W$ が成り立つ (定理 1.12 参照)．任意に Δ の元 r をとれば $r = w(s)$ をみたす $s \in \Pi, w \in W$ がある．したがって

$$\tau(r) = \tau w \tau^{-1}(\tau(s)) \in \Delta$$

を得る．すなわち $\tau(\Delta) = \Delta$ が成り立つ．

さて L の標準基を $\{h_p, e_r\}$ $(p \in \Pi, r \in \Delta)$ とおく．この時，適当に $\varepsilon_r = \pm 1$ を選べば $h_p \to h_{\sigma(p)}$, $e_r \to \varepsilon_r e_{\tau(r)}$ が L の自己同形に拡張できることを証明しよう．単純な複素 Lie 代数は Cartan 行列により一意的に定まるから $r \in \Pi$ について $e_r \to e_{\tau(r)}, e_{-r} \to e_{-\tau(r)}$ をみたす L の自己同形が存在する．それを ρ とおき $\rho(e_s) = \varepsilon_s e_{\tau(s)}$ $(\varepsilon_s = \pm 1)$ となることを証明しよう．まず $s \in \Delta^+$ と仮定し，s の高さ $\mathrm{ht}(s)$ について帰納法を用いる．定理 1.18 により

$$r = t + s, \quad t \in \Delta^+, \quad s \in \Pi, \quad \mathrm{ht}(t) < \mathrm{ht}(r)$$

をみたす t, s がある．帰納法の仮定により $\rho(e_t)=\varepsilon_t e_{\tau(t)}$ が成り立つ．さて $[e_t, e_s]=N_{t,s}e_{t+s}$ であるから

$$N_{t,s}\rho(e_r)=[\rho(e_t), \rho(e_s)]=[\varepsilon_t e_{\tau(t)}, e_{\tau(s)}]$$

となり $\rho(e_r)=\varepsilon_r e_{\tau(r)}$ を得る．ここで $\varepsilon_r=\varepsilon_t N_{\tau(t),\tau(s)}/N_{t,s}$ である．ところで Δ の根は同一の長さをもつから $t-s\notin\Delta$, したがって (2.6) により

$$N_{t,s}=\pm 1, \quad N_{\tau(t),\tau(s)}=\pm 1$$

を得るから ε_r は 1 または -1 となる．定義により $r\in\Pi$ ならば $\varepsilon_r=\varepsilon_{-r}=1$ が成り立つ．よって $[e_r, e_{-r}]=h_r$ より $\rho(h_r)=h_{\tau(r)}$ を得る．ところで任意の h_s は $\{h_r\}$ $(r\in\Pi)$ の整数係数一次結合となるから任意の s について $\rho(h_s)=h_{\tau(s)}$ が成り立つ．よって $\varepsilon_s=\varepsilon_{-s}$ を得る．

さて任意の体 F 上で定義された Δ 型普遍 Chevalley 群を G とおく．この時すべての $r\in\Delta$ について $\gamma(x_r(t))=x_{\tau(r)}(\varepsilon_r t)$ が成り立つ G の自己同形 γ があることを証明しよう．$\{x_{\tau(r)}(\varepsilon_r t)\}$ が G の生成元の間に成り立つ基本関係をみたすことを示せばよい(定理 8.6 の証明参照)．関係 (A) の成り立つことは明らかである．関係 (B) は (根の長さが一定だから) $r+s\in\Delta$ の時

$$[x_{\tau(r)}(\varepsilon_{.}\ \ ), x_{\tau(s)}(\varepsilon_s u)]=x_{\tau(r+s)}(\varepsilon_{r+s}N_{r,s}tu)$$

となる．左辺は $x_{\tau(r)+\tau(s)}(N_{\tau(r),\tau(s)}\varepsilon_r\varepsilon_s tu)$ に等しい．ところで ρ が L の自己同形だから $\rho([e_r, e_s])=[\rho e_r, \rho e_s]$ となる．よって

$$\varepsilon_{r+s}N_{r,s}=\varepsilon_r\varepsilon_s N_{\tau(r),\tau(s)}$$

を得て (B) が成り立つ．

さて $\varepsilon_r=\varepsilon_{-r}$ だから $\omega_r(t)\to\omega_{\tau(r)}(\varepsilon_r t)$ となる．よって $h_r(t)$ に対応する元は $h_{\tau(r)}(t)$ である．そこで関係 (C) の前半が成り立つ．後半も容易に証明される．たとえば第2の式は (6.9) に ρ を作用させた式を用いればよい．関係 (D) の成り立つこともすぐわかるので γ は普遍 Chevalley 群の自己準同形に拡張される．明らかに γ は全射である．一方，γ の位数は 2 または 3 であるから γ は自己同形となる． □

上に定義した γ を**グラフ型自己同形**という．次に体 F の自己同形を拡張して群の体型自己同形が得られることを示そう．

(10.2) 体 F の自己同形 θ に対応して $x_r(t)\to x_r(\theta(t))$ をみたす自己同形 $\varphi=\varphi_\theta$ が定まる．

証明 $V_F=F\otimes_Z\mathcal{V}$ に $\theta_1=\theta\otimes 1$ が定義される. θ の不変体を F_0 とおけば θ_1 は V_F の F_0 線形写像である. さて $\theta_1 x_r(t)\theta_1^{-1}=x_r(\theta(t))$ が成り立つ. したがって θ_1 による共役写像を φ とおけば (10.2) が成り立つ. ▯

根系 Δ は A_l, D_l, E_6 型のいずれかとし, 恒等写像でない自己同形を σ, その位数を n とする. D_4 型以外では $n=2$, D_4 型の時 $n=2$ または3である. 体 F は位数 n の自己同形 θ をもつと仮定する.

体 F 上の Δ 型普遍 Chevalley 群を G とし, σ が引きおこす E の等長写像を τ とおく. グラフ型自己同形 γ と体型自己同形 φ とは交換可能であるから

$$\rho(x_r(t))=x_{\tau(r)}(\varepsilon_r\theta(t))$$

とおけば $\rho=\gamma\varphi$ で ρ の位数は n となる. $\tau(\Pi)=\Pi, \tau(\Delta^+)=\Delta^+$ より ρ は部分群 $U=\langle X_r \mid r\in\Delta^+\rangle$ および $V=\langle X_{-r} \mid r\in\Delta^+\rangle$ を不変にする. そこで U の ρ 不変元の全体を U_1, V の ρ 不変元の全体を V_1 とし

$$G_1=\langle U_1, V_1\rangle$$

を Δ 型 Chevalley 群から導かれた **Steinberg 群**という.

あとで G_1 の中心による商群が一つの例外を除けばすべて単純群になることを証明する. そこで G_1 の中心に含まれる正規部分群を K とする時 G_1/K も Steinberg 群とよぶことにする. この節では普遍 Chevalley 群から出発したが任意の Chevalley 群から出発しても D_4 型で $n=3$ の場合を除けば G_1/K の形の Steinberg 群が得られる. このことを一応解説しておこう.

任意の Chevalley 群は G^u/Z という形をしている(定理8.6). 上に定義した G^u の自己同形 ρ はほとんどの場合 Z を不変にしている. これは G^u の中心が巡回群ならば明らかである. (群の中心および巡回群の部分群はすべて特性部分群である(『群論』上 p.48(6.13)). G^u の中心が巡回群でない場合は後節§10.3を参照されたい. Z が ρ 不変でないのは D_4 型で $n=3$ の場合だけである. さて ρ が Z を不変にすれば ρ は G^u/Z に自己同形 $\bar{\rho}$ を引きおこす. そこで $\bar{\rho}$ により不変となる U, V の元から生成される部分群として Steinberg 群が定義されるが, それは G_1/K と表わされる群と同形である.

2. A_l 型 Steinberg 群　A_l 型の Chevalley 群からユニタリ群が得られることを証明しよう. A_l 型の Lie 代数は $n=l+1$ 次で対角和が0となる行列の全体がつくる Lie 代数である. そこで n 次元線形空間の基を $\{e_0, \cdots, e_l\}$

とおけば $\Delta=\{e_i-e_j\}$ $(i\neq j)$ が A_l 型の根系で

$$\{e_{i-1,i-1}-e_{ii}\ (i=1,\cdots,l), e_{ij}\ (i\neq j)\}$$

が Lie 代数の標準基となる(§3.1). ここで $\{e_{i-1,i}\ (i=1,2,\cdots,l)\}$ が Δ の基本系に対応している. Dynkin の図形の自己同形 σ は中点による対称だから σ が引きおこす Lie 代数の自己同形により $e_{jk}\leftrightarrow \pm e_{l-k,l-j}$ となる. さて逆対角行列 A を次のように定義する.

$$A=\varepsilon\sum(-1)^i e_{i,l-i},$$

ここで和は i について 0 から l まで, ε は l が偶数ならば $\varepsilon=1$ でよいが l が奇数の場合は $\theta(\varepsilon)=-\varepsilon\neq 0$ をみたす元 ε をとる. この時

$$\alpha: M\longmapsto -A^{-1}({}^tM)A$$

は Lie 代数の自己同形となる. これが σ の拡張となることは容易に示される.

前に注意したように A_l 型の場合, 自然な表現による一般 Chevalley 群は普遍的である(§8.2 最後の注意). よって G を $SL(V)$ と同一視する. $r=e_i-e_j$ に対応する $x_r(t)$ は $I+te_{ij}$ (I は (n,n) 型単位行列) であるから

$$\rho(x_r(t))=I+\varepsilon_r\theta(t)e_{l-j,l-i} \qquad (\varepsilon_r=(-1)^{i+j+1})$$

となる. よって ρ は $M\longmapsto A^{-1}\theta({}^tM)^{-1}A$ と一致する. そこで ρ による不変元 M は ${}^tM\theta(A)\theta(M)=\theta(A)$ をみたしている $(\theta^2=1)$. さて $\theta(A)$ に対応する形式を h とおけば, $\theta(A)={}^tA$ が成り立つから, h は Hermite 形式である. そして M は h に対応するユニタリ群 $U(h)$ の元となる. したがって A_l 型の Steinberg 群 G_1 は $\langle U_1, V_1\rangle$, すなわち $U(h)$ の中でベキ単3角行列全体が生成する部分群である. 以下 $G_1=SU(h)$ を証明しよう.

形式 h の定義から基の元 e_0 は等方的である. ここで任意に等方的な元 v をとれば $\sigma(v)\in\langle e_0\rangle$ をみたす G_1 の元 σ が存在することを証明しよう. まず $l=2m$ と偶数になる場合を考える. そこで $m=1$ の時 $v=\alpha e_0+\beta e_1+\gamma e_2$ とおけば $h(v,v)=\alpha\theta(\gamma)-\beta\theta(\beta)+\gamma\theta(\alpha)$ となる. よって $\gamma=0$ ならば, v が等方的だから $\beta=0$ を得る. よって $v\in\langle e_0\rangle$ が成り立つ. もし $\gamma\neq 0$ ならば v の代りに $\gamma^{-1}v$ を考え, $\gamma=1$ と仮定してよい. この時

$$\sigma_1=\begin{pmatrix}1 & \theta(\beta) & \alpha\\ 0 & 1 & \beta\\ 0 & 0 & 1\end{pmatrix}$$

は G_1 の元で $\sigma_1(e_2)=v$ が成り立つ．一方，$\langle e_0, e_2\rangle$ は双曲型平面だから定理 Ⅱ 6.2 により $\sigma_2(e_2)\in\langle e_0\rangle$ をみたす G_1 の元 σ_2 がある．したがって $\sigma_2\sigma_1{}^{-1}=\sigma$ により $\sigma(v)\in\langle e_0\rangle$ となる．一般の場合には

$$\theta(A)=\begin{pmatrix} & & J' \\ & a & \\ J & & \end{pmatrix},\quad T=\begin{pmatrix} A & & \\ & 1 & \\ & & C \end{pmatrix}$$

とおく．ここで $J'={}^tJ$ は (m, m) 型の逆対角行列，空所は 0 である．さて T において $A\in SL(m, F), {}^tC^{-1}=J\theta(A)J^{-1}$ ならば T は $U(h)$ の元である．定理 Ⅱ 2.7 により T はベキ単 3 角行列の積となる．よって $T\in G_1$ が成り立つ．また I を $(m-1, m-1)$ 型の単位行列として S を

$$S=\begin{pmatrix} I & & \\ & P & \\ & & I \end{pmatrix}$$

という形の行列で P が 3 次元のユニタリ群のベキ単 3 角行列の積となる元とすれば $S\in G_1$ となる．等方的元 $v=\sum\alpha_i e_i$ において $\alpha_i=0\ (i>m)$ とすれば $\alpha_m=0$ を得る．したがって Ⅰ (2.11) により適当に $T\in G_1$ を選べば $T(v)$ が $\langle e_0\rangle$ の元となる．いま $\alpha_i\ (i>m)$ のうち 0 でないものがあれば，適当に C を選んで $T_1\in G_1$ を定義すれば

$$T_1(v)=u+\alpha e_{m-1}+\beta e_m+\gamma e_{m+1}\qquad (u\in\langle e_0, \cdots, e_{m-2}\rangle)$$

となる．3 次元の場合を用いれば $T_1(v)$ を $u+\alpha' e_{m-1}$ に移すことができる．よって適当に G_1 の元 σ をとって $\sigma(v)\in\langle e_0\rangle$ とすることができる．

l が奇数の場合も同様である．この場合 $\theta(A)$, T では中央の行，列を省き，$J'=\theta({}^tJ)$ とした上で，S には中央に 2 次元の行列 P をおけばよい．定理 Ⅱ 6.2 により 2 次元の場合には命題が成り立つから上と同様に一般の次元について $\sigma(v)\in\langle e_0\rangle$ をみたす G_1 の元 σ が存在する．

さて $U(h)$ に含まれるユニタリ移換を τ とすれば Ⅱ (6.3) により

$$\tau(x)=x+\gamma h(x, v)v$$

をみたす等方的元 v がある．上に証明したように $\sigma(v)\in\langle e_0\rangle$ をみたす G_1 の元 σ がある．$\sigma\tau\sigma^{-1}$ はユニタリ移換で

$$\sigma\tau\sigma^{-1}(x)=x+\gamma' h(x, e_0)e_0$$

となる．一方，$h(e_i, e_0)=0$ $(i<l)$ が成り立つから $\sigma\tau\sigma^{-1}$ はベキ単上3角行列で G_1 の元である．したがって $\tau\in G_1$ を得る．すなわち G_1 はすべてのユニタリ移換を含むから定理 II 6.4 により $G_1\supset SU(h)$ を得る．逆の包含関係は明らかに成り立つ．よって $G_1=SU(h)$ が成り立つ．

注意 Steinberg 群として現われるユニタリ群は極大指数のものだけである．また極大指数で同次元のユニタリ群は同形である． ▯

3. D_l 型の古典型 Steinberg 群 D_l 型の Steinberg 群 $(\sigma^2=1)$ は指数 $l-1$ の直交群の交換子群を中心で割った商群であることを証明しよう．D_l 型の単純 Lie 代数は $L(J)$ と表わされる．その標準基として§3で求めたものを用いる．基本系の元に対応するものは $u_{12}, u_{23}, \cdots, u_{l-1,l}, s_{l-1,l}$ である．$L(J)$ の自己同形で最初の $l-2$ 個は動かず，最後の二つが交換される．ところで $u_{ij}=e_{ij}-e_{l+j,l+i}, s_{l-1,l}=e_{l-1,2l}-e_{l,2l-1}$ だからこの $L(J)$ の自己同形は l 番目の座標と $2l$ 番目の座標を交換する写像により得られる．その座標変換の行列を A とおけば $L(J)$ の任意の元 M について

$$M\longmapsto AMA^{-1}$$

が σ の引きおこす自己同形と一致する．さて

$$Q(\sum\lambda_i y_i)=\lambda_1\lambda_{l+1}+\cdots+\lambda_l\lambda_{2l}$$

と2次形式 Q を定義すれば，$L(J)$ の自然表現による Chevalley 群は直交群の交換子群 $\Omega(Q,F)$ である(§3参照)．体 F 上の D_l 型普遍 Chevalley 群を G^u とおく．(G^u はいわゆるスピン群 Spin (Q,F) である．) F の標数が2ならば $G^u=\Omega(Q,F)$ であるが F の標数が2でなければ定理8.10により G^u の中心に含まれる位数2の部分群 Z があって $\Omega(Q,F)\cong G^u/Z$ となっている．(自然表現に関する重みの生成する格子 Γ_V は Q の中で指数2の部分群である(§8.2節末の注意参照).) §10.1で述べたように G^u の自己同形 ρ が定義され Steinberg 群 $G_1=\langle U_1, V_1\rangle$ が定まる．ここで ρ が Z を不変にすることを示そう．Z は H の部分群である．定理8.3により

$$\prod h_i(t_i)\in Z \Longleftrightarrow \text{すべての } \mu\in\Gamma_V \text{ について } \prod t_i^{\mu(h_i)}=1$$

が成り立つ．§8.2の節末の注意1において Γ_V の生成集合を Q の基 $\{q_i\}$ を用いて表わしてあるからその結果を用いて

$$\prod h_i(t_i)\in Z \Longleftrightarrow t_1=\cdots=t_{l-2}=1, t_{l-1}t_l=t_{l-1}^{-1}t_l=1$$

を得る．すなわち $t_1=\cdots=t_{l-2}=1, t_{l-1}=t_l=\pm 1$ となる．ρ は $h_r(t)$ を $h_{\tau(r)}(t)$ に動かすから ρ は Z を不変にする．

さて ρ は $\Omega(Q,F)$ に自己同形を引おこす．これは $\Omega(Q,F)$ の元 M に

$$M \longmapsto A\theta(M)A^{-1}$$

と作用している．自然表現による Steinberg 群は $\theta(M)=A^{-1}MA$ をみたすベキ単 3 角行列から生成される部分群 $G_2\subset\Omega(Q,F)$ である．したがって G_2 の生成元は §5.5 の記号を用いて

$$\begin{array}{ll} I+tu_{ij},\quad I+ts_{ij} & (i<j<l, t\in F_0 \ (F_0 \text{ は } \theta \text{ の不変体})) \\ (I+\alpha u_{il})(I+\theta(\alpha)s_{il}) & (i<l) \\ I+su_{ji},\quad I+st_{ij} & (i<j<l,\ s\in F_0) \\ (I+\alpha u_{li})(I+\theta(\alpha)t_{il}) & (i<l) \end{array}$$

となる．さて $F=F_0(\zeta)$ とおき ζ のみたす F_0 上の既約多項式を

$$X^2+aX+b=0 \qquad (a,b\in F_0)$$

とする．行列の作用している空間 V の座標を $\{y_i\}$ から $\{x_i\}$ に

$$x_i=y_i\ (i\neq l, 2l),\quad x_l=y_l+y_{2l},\quad x_{2l}=-\zeta y_l-\theta(\zeta)y_{2l}$$

と変換する．この座標変換の行列を S とおけば

$$SG_2S^{-1}\subset S\Omega(Q,F)S^{-1}=\Omega(Q',F)$$

となる．2 次形式 Q' は $Q'(v)=Q(S^{-1}v)$ により定義される．ところで

$$v=\sum\lambda_iy_i=\sum\mu_ix_i$$

ならば $\mu_i=\lambda_i\ (i\neq l, i\neq 2l)$ および $\lambda_l=\mu_l-\zeta\mu_{2l}, \lambda_{2l}=\mu_l-\theta(\zeta)\mu_{2l}$ が成り立つ．よって $Q'(\sum\mu_ix_i)$ は（ζ のみたす既約式の係数 a,b を用いて）

$$\mu_1\mu_{l-1}+\cdots+\mu_{l-1}\mu_{2l-1}+\mu_l{}^2+a\mu_l\mu_{2l}+b\mu_{2l}{}^2$$

となる．G_2 の元は $\theta(M)=A^{-1}MA$ をみたすから SG_2S^{-1} の元について

$$\theta(SMS^{-1})=\theta(S)A^{-1}MA\theta(S)^{-1}$$

が成り立つ．ところで行列 S は $\theta(S)A^{-1}=S$ をみたす．よって $M'\in SG_2S^{-1}$ は $\theta(M')=M'$ を満足する．すなわち SG_2S^{-1} は F_0 上の行列のつくる群で

$$SG_2S^{-1}\subset\Omega(Q',F)\cap O(Q',F_0)$$

が成り立つ．多項式 X^2+aX+b は F_0 上既約，そしてその零点により F が生成されるから，Q' の形からその指数は F_0 上で $l-1$，F 上で l となる．以下

$$SG_2S^{-1}=\Omega(Q',F_0)$$

を証明しよう．さて行列の計算により G_2 の生成元は G_2 の中で交換子となっていることが証明される．したがって $SG_0S^{-1}\subset\Omega(Q',F_0)$ を得る．また行列の計算により，SG_2S^{-1} の元により線形空間 $\sum F_0x_i$ の非特異元を $x_1+\lambda x_{l+1}$ にうつせることが示される．D_l 型の Chevalley 群の場合と同様に

$$SG_2S^{-1}\supset\Omega(Q',F_0)$$

が証明されるので $SG_2S^{-1}=\Omega(Q',F_0)$ が成り立つ．

注意　D_4 で σ の位数が3の場合には ρ は $\{h_i(t)\}$ に位数3の置換を引きおこす．よって体 F の標数が奇数の場合，自然表現に対応する群では部分群 Z は ρ 不変でない．この場合 $\Omega(Q,F)$ は ρ に相当する自己同形をもたない．▯

§11　Steinberg 群の構造

1. 部分群 N_1, H_1 および Weyl 群 W_1　　この節では§10.1の記号を襲用する．根系 Δ は A_l, D_l, E_6 型のいずれかとし，その図形の，恒等写像ではない自己同形を σ とする．(10.1) により σ は Δ の置換 τ を引きおこし

(11.1)
$$\tau(\Delta^+)=\Delta^+$$

が成り立つ．すなわち τ は根の符号を変えない．Δ 型 Lie 代数 L_F は

$$h_p\longrightarrow h_{\sigma(p)},\qquad e_r\longrightarrow \varepsilon_r e_{\tau(r)}\quad(\varepsilon_r=\pm1)$$

をみたす自己同形をもっている．この自己同形と体 F の自己同形 θ を組み合わせて F 上の Δ 型普遍 Chevalley 群 G の自己同形 ρ が定義され

(11.2)
$$\rho(x_r(t))=x_{\tau(r)}(\varepsilon_r\theta(t))$$

が成り立つ．この節を通じて上の記号を用い，さらに θ の不変体と F_0 とおく．まず次の補題を証明しよう．

(11.3)　G の部分群 U, V, B, N, H を§7で定義した通りとすれば ρ はこれらの部分群を不変にする．また元 $\omega_r(t), h_r(t)$ も§7.3の定義通りとすれば次の公式が成り立つ．

$$\rho(\omega_r(t))=\omega_{\tau(r)}(\varepsilon_r\theta(t)),\qquad \rho(h_r(t))=h_{\tau(r)}(\theta(t)).$$

証明　(11.1) および (11.2) により $\rho(U)=U$ が成り立つ．V についても同様である．定理7.27により $B=N_G(U)$ となるから ρ は B も不変にする．グラフ型の自己同形 γ が $h_r(t)$ を $h_{\tau(r)}(t)$ に移すことは (10.1) の証明中で示されている．よって ρ について上の公式が成り立つ．$\omega_r(t)$ についても同様であ

る．これらの式から ρ が部分群 N, H を不変にすることがわかる． □

自己同形 ρ が N も H も不変にするから ρ は Weyl 群 $W=N/H$ の自己同形を引きおこす．この W の自己同形も ρ と表わすことにする．(7.8) により $H\omega_r$ に対応する Weyl 群の元が w_r であるから

$$\text{(11.4)} \qquad \rho(w_r)=w_{\tau(r)}$$

が成り立つ．さて，W_1, N_1, H_1 を次のように定義する．

定義 11.5 W の元で ρ 不変なもの全体のつくる部分群を W_1 とおく．ρ が定める Steinberg 群を $G_1=\langle U_1, V_1\rangle$ とし N_1, H_1 を次式により定める．

$$N_1=G_1\cap N, \qquad H_1=G_1\cap H. \quad □$$

まず W_1 の構造を調べよう．

(11.6) σ に関する Π 上の軌道の一つを J とおき，J から生成される正根の全体を J^+ と表わす．この時 J^+ は

$$\{r\} \quad (r=\sigma(r)), \qquad \{r, \sigma(r)\} \quad (r \text{ と } \sigma(r) \text{ は直交する})$$

$$\{r, \sigma(r), \sigma^2(r)\} \text{ (互いに直交)}, \qquad \{r, \sigma(r), r+\sigma(r)\} \quad (A_2 \text{ 型})$$

のいずれかと一致する．(それぞれ $A_1, A_1{}^2, A_1{}^3, A_2$ 型という．)

証明 各図形に対応する σ の作用から明らかである．A_2 型は l が偶数の時 A_l 型の群に現われる． □

さて Π 上の任意の σ 軌道を J とし $W(J)=\langle w_r | r\in J\rangle$ とおく．前のように Euclid 空間 E を定義して，W を E の等長写像の群と考える．(10.1) により τ も E の等長写像である．ここで次の補題が成り立つ．

(11.7) 上の記号の下で $\rho(w)=\tau w\tau^{-1}$ が成り立つ．また

$$W_1(J)=W_1\cap W(J)$$

とおけば $W_1(J)=\{1, w_0(J)\}$ となる．ここで $w_0(J)$ は J の各根の符号を変えるが Δ^+-J^+ の元の符号を変えない位数 2 の元である．$W(J)$ は J の各根の符号を変える元を唯一つ含んでいる．根系 Δ のすべての元の符号を変える W の元を w_0 とおけば w_0 は W_1 の元である．((1.14)(b) 参照．)

証明 (11.4) により任意の $r\in\Delta$ について $\rho(w_r)=\tau w_r\tau^{-1}$ が成り立つ．ところで W は w_r $(r\in\Delta)$ により生成されるから $\rho(w)=\tau w\tau^{-1}$ がすべての $w\in W$ について成り立つ．

J が生成する根系に (1.14) を適用すれば J に含まれる各根の符号を変える

元が $W(J)$ の中に唯一つ存在することがわかる．この元を w_1 とおけば定理1.13により w_1 は J^+ 以外の正根の符号は変えない．さて J は σ による軌道だから $r\in J\Rightarrow\sigma(r)\in J$ が成り立つ．よって $\tau W(J)\tau^{-1}=W(J)$ を得る．特に $\tau w_1\tau^{-1}\in W(J)$ となる．$\tau w_1\tau^{-1}$ も J の任意の根を負根に移すから w_1 の一意性により $\tau w_1\tau^{-1}=w_1$ が成り立つ．よって $\rho(w_1)=w_1$ となり w_1 は $W_1(J)$ の元となる．同様に (11.7) の最後の主張も成り立つ．

いま $W_1(J)$ の任意の元 w をとり $w\neq1$ と仮定する．この時 w は少なくとも一つの J の元の符号を変える(定理1.13)．そこで $w(r)<0$ と仮定すれば $w(\tau(r))=\tau(w(r))<0$ が成り立つ((11.1)および $w=\rho(w)$)．J は σ 軌道だから w は J の各元の符号を変える．したがって $w=w_0(J)$ となり，(11.7) が証明される．□

(11.8)　W_1 は $w_0(J)$ (J は Π の σ 軌道全体を動く) により生成される．

証明　w により負となる正根の数を $n(w)$ とおき，$n(w)$ に関する帰納法により $w\in W_1$ が $w_0(J)$ の積として表わされることを証明しよう．$w=1$ の場合は明らかであるから $w\neq1$ と仮定する．この時 w は少なくとも一つの Π の元 r の符号を変える．r を含む σ 軌道を J とおけば，(11.7) の証明と同様に w は J の各元の符号を変える．さて，$w_0(J)$ は J の各元の符号を変えるが，Δ^+-J^+ に含まれる根の符号は変えない．したがって

$$n(w_0(J)w)=n(w)-|J^+|$$

となる．帰納法の仮定により $w_0(J)w=w_0(J_1)\cdots w_0(J_k)$ を得るから w も $w_0(J_i)$ という形の元の積となる．□

次の命題により W_1 の構造が明らかとなる．

(11.9)　Π の元が生成する Euclid 空間を E とし，E の元 v に対し τ 軌道上の平均を $a(v)$ とおく．すなわち $\tau(v)\neq v$ ならば

$$a(v)=(v+\tau(v))/2 \quad または \quad a(v)=(v+\tau(v)+\tau^2(v))/3$$

である．さらに $E_1=\{v\in E\,|\,\tau(v)=v\}$ とおく．W_1 は E_1 の線形写像のつくる群となる．いま Π 上の σ 軌道の一つを J とし，J の1元を r とすれば E_1 の写像として $w_0(J)$ は $a(r)$ に関する対称変換と一致する．根系 Δ が A_l, D_l ($\sigma^2=1$), D_4 ($\sigma^3=1$), E_6 型に応じて W_1 は C_k, B_{l-1}, G_2, F_4 型の Weyl 群と同形になる．

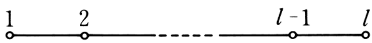
(ここで A_l 型の場合 $k=l/2$ または $k=(l+1)/2$ となる.)

証明　明らかに E_1 は $\{a(r)\}$ $(r\in\Pi)$ が生成する部分空間である. いま任意に $w\in W_1, v\in E_1$ をとれば $\tau w=w\tau$ だから $\tau(w(v))=w(v)$ が成り立つ. すなわち w は E_1 に作用している. ところで $w\neq 1$ ならば w により符号の変わる Π の元 r がある. $w\in W_1$ だから w は $\tau(r)$ の符号も変えるので $w(a(r))<0$ となる. よって w は E_1 の正元を負に移すから, E_1 の写像として恒等写像ではない. したがって W_1 は E_1 の線形写像の群となる.

さて (11.9) のように J, r をとれば $w_0(J)$ は J の各元の符号を変える. よって $w_0(J)a(r)=-a(r)$ となる. 一方, E_1 の元 v が $a(r)$ と直交していれば τ が等長写像であることから $(v,r)=(v,\tau(r))=(v,a(r))=0$ を得る. $w_0(J)$ は $w_r, w_{\tau(r)}$ (および $w_{\tau^2(r)}$) から生成される群の元だから v を不変にする. すなわち $(v,a(r))=0\Rightarrow w_0(J)v=v$ となり E_1 上で, $w_0(J)$ は $a(r)$ に関する対称変換と一致する.

対称変換が生成する有限群は Coxeter 群で, その構造は $\{a(r)\}$ の間の角により定まる(『群論』上 p. 354). この場合 Δ の型に応じて§3のように根系を定めれば $\{a(r)\}$ を求めることができて W_1 の構造がわかる. 各場合に実行してみよう.

A_l $(l=2k-1$ は奇数$)$. $\Pi=\{r_1,r_2,\cdots,r_l\}$ が



に対応していれば $a(r_1)=(r_1+r_l)/2,\cdots,a(r_k)=r_k$ となる. したがって $a(r_1),\cdots,a(r_k)$ は C_k 型の基本系と同形である.

l が偶数の場合には$(l=2k)$, $a(r_k)=(r_k+r_{k+1})/2$ となり, B_k 型の基本系と同形になる. B_k 型でも C_k 型でも Weyl 群は同形である.

D_l $(\tau^2=1)$. この場合 $a(r_i)=r_i$ $(i\leqq l-2)$ で $a(r_{l-1})=(r_{l-1}+r_l)/2$ となる. よって $\{a(r_i)\}$ は B_{l-1} 型の基本系と同形である.

D_4 $(\tau^3=1)$. この場合§3.4の記号で $a(r_1)=(r_1+r_3+r_4)/3, a(r_2)=r_2$ となる. よって W_1 は G_2 型である.

E_6 の場合も同様で W_1 は F_4 型になる. ▯

(11.10)　Δ の元 s を任意にとる. この時 W_1 の元 w と Π の σ 軌道 J が存

在して $w(s)\in J^+$ となる．

証明 $s\in\Delta^+$ と仮定してよい．Δ^+ の各元の符号を変える元を w_0 とおけば (11.7) により w_0 は W_1 の元である．よって Π の σ 軌道 $J_1,\cdots,J_k$ があって ((11.8)参照) $w_0=w_0(J_1)\cdots w_0(J_k)$ と表わすことができる．ところで $w_0(s)<0$ だから定理1.13の証明と同様に $w\in W_1$ と σ 軌道 J があって

$$w(s)>0,\quad w_0(J)w(s)<0$$

となる．$w_0(J)$ が符号を変える正根は J^+ の元に限るから $w(s)\in J^+$． □

注意 根系 Δ に対し $a(\Delta)=\{a(r)\,|\,r\in\Delta\}$ と定義すれば $a(\Delta)$ は§1に述べた根系の条件のうち (1.2)(i)—(iv) をみたしている．条件 (i), (ii) をみたすことは明らかである．(11.9) および (11.10) により (iii) も成り立つ．条件 (iv) は各型に応じて計算により確かめることができる．

l が偶数で A_l 型の場合を除けば $a(\Delta)$ は条件 (v) もみたし根系となる．これらの場合には W_1 が根系 $a(\Delta)$ の Weyl 群と一致する．A_{2k} 型の場合は σ 軌道に A_2 型のものが現われる．この時 A_2 型軌道を $\{r,\sigma(r)\}$ とすれば $J^+=\{r,\sigma(r),r+\sigma(r)\}$ となり $2a(r)=a(r+\sigma(r))$ を得る．よって条件 (v) は成り立たない．$a(\Delta)$ は "BC_k 型の根系" と呼ばれるもので正規直交系 $\{e_i\}$ をとった時 $\{\pm e_i\pm e_j\ (i\neq j), \pm e_i, \pm 2e_j\}$ $(i,j=1,2,\cdots,k)$ で与えられる． □

2. Steinberg 群の Tits 系 Π の σ 軌道の一つを J とすれば自己同形 ρ は

$$U(J)=\langle X_r\,|\,r\in J\rangle$$

を不変にする(11.3)．そこで ρ 不変な $U(J)$ の元全体のつくる集合を $U_1(J)$ とおく．その構造を J の型別にわけて調べよう．

(11.11) J の元 r を定める．

その上で J が $A_1{}^i$ 型の場合 $i=1,2,3$ に応じてそれぞれ $x_J(t)$ を $x_r(t)$ (A_1 型，$\theta(t)=\varepsilon_r t$), $x_r(t)x_{\tau(r)}(t')$，または $x_r(t)x_{\tau(t)}(t')x_{\tau^2(t)}(t'')$ (ここで $t\in F^\#, \varepsilon_r$ は(11.2)の定数，$t'=\varepsilon_r\theta(t), t''=\varepsilon_r\varepsilon_{\tau(r)}\theta^2(t)$) とおく．$J$ が A_2 型の場合は

$$u+\theta(u)=-\varepsilon_r N_{r,\tau(r)}t\theta(t)$$

($N_{r,\tau(r)}$ は (2.2) で定義される Lie 代数の乗法定数) をみたす t,u をとり

$$x_J(t,u)=x_r(t)x_{\tau(r)}(t')x_s(u)\qquad (s=r+\tau(r))$$

とおく．この時 $U_1(J)=\{x_J(t)\}$ または $\{x_J(t,u)\}$ となり

$$x_J(t_1)x_J(t_2)=x_J(t_1+t_2)$$
$$x_J(t_1,u_1)x_J(t_2,u_2)=x_J(t_1+t_2,v)$$

$(v=u_1+u_2+\varepsilon_r N_{r,\tau(r)}\theta(t_1)t_2)$ が成り立つ．

証明　$A_1{}^i$ 型の場合はいずれも同様だから $i=2$ の場合を証明しよう．まず $\rho^2=1$ だから $\varepsilon_r\varepsilon_{\tau(r)}=1$ となる．定理 7.3 により $U(J)$ の元は

$$x_r(t)x_{\tau(r)}(u)$$

という形に一意的に書ける．この場合 $r+\tau(r)\notin\Delta$ だから X_r と $X_{\tau(r)}$ とは元別に交換可能である．そこで $\rho(x_r(t)x_{\tau(r)}(u))=x_r(t)x_{\tau(r)}(u)$ より

$$\varepsilon_r\theta(t)=u$$

を得る．したがって $U_1(J)=\{x_J(t)\,|\,t\in F^{\#}\}$ となる．A_1 型の場合には t に $\theta(t)=\varepsilon_r t$ という制限がつく．乗法公式は X_r と $X_{\tau(r)}$ とが元別に可換だから明らかに成立する．

A_2 型の軌道の場合は $J^+=\{r,\tau(r),s\}$ $(s=r+\tau(r))$ だから定理 7.3 により $U(J)$ の元 x は $x=x_r(t)x_{\tau(r)}(u)x_s(v)$ という形に一意的に書ける．この場合 X_s は $U(J)$ の中心に含まれている．さらに

$$[x_r(t),x_{\tau(r)}(u)]=x_s(N_{r,\tau(r)}tu)$$

が成り立つ．この場合も $\varepsilon_r\varepsilon_{\tau(r)}=1$ となるが $\varepsilon_s=-1$ が成り立つ．これは $[e_r,e_{\tau(r)}]=N_{r,\tau(r)}e_s$ の両辺に Lie 代数の自己同形を適用すれば容易に証明される．そこで $\rho(x)=x$ となるための条件は

$$u=\varepsilon_r\theta(t),\quad v+\theta(v)=-\varepsilon_r N_{r,\tau(r)}t\theta(t)$$

である．乗法公式も定理 7.1 を用いて証明される．□

さて $V(J)=\langle X_{-r}\,|\,r\in J\rangle$ とおけば $V(J)$ の ρ 不変元の集合 $V_1(J)$ について (11.11) と同様の結果が成り立つ．

(11.12)　(7.8) において定義された N/H から W の上への同形写像を f とおく．もし $w\in W_1$ ならば $f(Hn)=w$ をみたす N_1 の元が存在する．よって f により N_1/H_1 が W_1 と同形になる．

証明　N_1 の任意の元 n は $\rho(n)=n$ をみたすから Hn は ρ 不変である．したがって f は N_1/H_1 から W_1 の中への同形写像となる．f が W_1 の上への写像であることを証明しよう．W_1 は $w_0(J)$ により生成される ((11.8) 参照) から任意の J について $f(Hn)=w_0(J)$ をみたす $n\in N_1$ があることを証明すればよい．さて (11.11) を $V_1(J)$ に適用すれば $V_1(J)\neq\{1\}$ となる．いま $V_1(J)$ の元 x をとり $x\neq1$ と仮定する．その標準形を $x=unv$ とおく (定理 7.25)．すなわち $u\in U,n\in N,f(Hn)=w,v\in U_w^-$ が成り立ち (u,n,v) は一意的に定ま

る．さて $\rho(x)=x$ だから $x\in B\rho(n)B$，したがって $f(H\rho(n))=w$ を得る．ゆえに $w=\rho(w)\in W_1$ となる．一方，$x\in V_1(J)$ だから $w\in W(J)$ も成り立ち，$w\in W_1\cap W(J)=W_1(J)$ となる．(11.7) により $w=1$ または $w=w_0(J)$ である．ところで $w=1$ ならば $x\in U\cap V_1(J)=\{1\}$ となり x の定義に矛盾する．よって $w=w_0(J)$ となる．

一般に $w\in W_1$ ならば ρ は U_w^- を不変にする．(いま w の代表元 z を N から選べば $\rho(z)$ も w を代表する元であるから

$$\rho(U_w^-)=\rho(U\cap zVz^{-1})=U\cap\rho(z)V\rho(z)^{-1}=U_w^-$$

が成り立つ．§7.6 参照.）そこで $x=\rho(x)=\rho(u)\rho(n)\rho(v)$ となるが，標準形の一意性により (定理 7.25)，$\rho(u)=u, \rho(n)=n, \rho(v)=v$ を得る．よって $x\in V_1$, $u\in U_1, v\in V_1$ が成り立つ．また $n\in N\cap G_1=N_1$ となる．さらに $f(Hn)=w=w_0(J)$ も成り立ち，(11.12) が証明される．▯

(11.13)　G_1 の元 x の標準形を $x=unv$ とすれば

$$u\in U_1,\quad n\in N_1,\quad v\in U_1\cap U_w^-$$

が成り立つ．また $w=f(Hn)$ は W_1 の元である．

証明　(11.12) の証明と同様に $f(Hn)=w\in W_1$ を得るから ρ は U_w^- を不変にする．したがって (11.12) の証明と同様にしてこの命題が証明される．▯

定理 11.14　Steinberg 群 G_1 について $B_1=U_1H_1, S_1=\{w_0(J)\}$ (ここで J は Π の σ 軌道全体を動く）とおく．この時 (G_1, B_1, N_1, S_1) は G_1 の Tits 系である (§7.4 参照).

証明　基本系 Π の各元の符号を変える W の元を w_0 とおく．w_0 は W_1 の元であるから $f(Hn_0)=w_0$ をみたす N_1 の元 n_0 がある (11.12)．(9.2) により $n_0Un_0^{-1}=V$ となる．ところで $n_0\in N_1$ だから

$$n_0U_1n_0^{-1}=G_1\cap n_0Un_0^{-1}=V_1$$

が成り立つ．すなわち $G_1=\langle U_1, V_1\rangle=\langle B_1, N_1\rangle$ を得る．

明らかに $B_1\cap N_1\supset H_1$，一方 $B_1\cap N_1\subset B\cap N\cap N_1=H\cap N_1=H_1$ だから

$$H_1=B_1\cap N_1\lhd N_1$$

となり条件 (T1) が成り立つ．

命題 (11.8) および (11.12) から条件 (T2) の成り立つことが証明される．

次に条件 (T3)′ が成り立つことを証明しよう．そこで J を Π の σ 軌道とす

れば $w_0(J)$ は w_r $(r\in J)$ の積として表わされる．したがって (7.13) により任意の $w\in W_1$ に対して

$$(B_1w_0(J)B_1)(B_1wB_1)\subset\bigcup BzwB$$

となる．ここで上式の右辺は $z\in W(J)$ についての和集合である．左辺は G_1 の部分集合である．さて両側剰余類 BuB $(u\in W)$ が G_1 の元を含んでいると仮定すれば (11.13) により $u\in W_1$ を得る．よって上の包含式の右辺において $zw\in W_1$ と制限してよい．$w\in W_1$ だから z は $W_1\cap W(J)$ の元を動く．よって (11.7) から $z=1$ または $z=w_0(J)$ となる．よって

$$w_0(J)B_1w\subset B_1wB_1\cup B_1w_0(J)wB_1,$$

すなわち (T3)′ が成り立つ．

最後に $w_0(J)B_1w_0(J)$ は $V_1(J)\neq\{1\}$ を含むから (T4) も成り立つ．よって G_1 は Tits 系 (G_1, B_1, N_1, S_1) をもっている．□

3. 部分群 H_1 の構造　部分群 H_1 の構造は G が普遍 Chevalley 群の場合が一番簡明である．

(11.15) G を普遍 Chevalley 群とする．Π における σ 軌道の一つを J とする．いま $J=\{r\}$ の場合は $t\in F_0^\#$ について $h_J(t)=h_r(t)$ とおく．$|J|>1$ の場合には $r\in J$ を一つ定めて $h_J(\alpha)=h_r(\alpha)h_{\sigma(r)}(\theta(\alpha))$ $(\alpha\in F^\#)$ または $h_J(\alpha)=h_r(\alpha)h_{\sigma(r)}(\theta(\alpha))h_{\sigma^2(r)}(\theta^2(\alpha))$ とおく．ρ 不変な H の元は

$$\prod h_J(t_J)\qquad (J \text{ は } \Pi \text{ の } \sigma \text{ 軌道全部を動く})$$

と一意的に表わされる．

証明　(8.4) により H の元 h は $h=\prod h_i(t_i)$ $(t_i\in F^\#)$ と一意的に表わされる．$\rho(h)=h$ ならば (11.3) により $r_j=\tau(r_i)\Rightarrow t_j=\theta(t_i)$ が成り立つ．よって ρ 不変な元は $\prod h_J(t_J)$ という形に書くことができる．この表現が一意的であることは明らかである．□

定理 11.16 G_1 を普遍 Chevalley 群から得られる Steinberg 群とする．この時 ρ 不変な H の元全体のつくる集合を H_2 とおけば $H_1=H_2$ となる．すなわち，H_1 の元は $\prod h_J(t_J)$ と一意的に表わすことができる．

証明　定義により $H_1\subset H_2$ は明らかに成り立つ．よって定理を証明するには H_2 の生成元がすべて H_1 に含まれていることを示せばよい．

さて，任意の $r\in\Pi$ について $G_r=\langle x_r(t), x_{-r}(s)\rangle$ $(t, s\in F)$ とおく．(8.7)

により $G_r \cong SL(2, F)$ となる．この同形対応は

$$x_r(t) \longmapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad x_{-r}(s) \longmapsto \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}$$

によって与えられる．いま Π の σ 軌道 J をとれば(11.6)により J の型が定まる．$|J|>1$ の場合は J の元 r を一つ定めて $x_J(t), h_J(t)$ をそれぞれ (11.11), (11.15) により定義し，$x_{-J}(t)$ を $x_{-J}(t)=x_{-r}(t)x_{-\tau(r)}(t')$ $(t'=\varepsilon_r\theta(t))$ などと定義する．まず $J=\{r\}$ と仮定しよう．この時 ρ は G_r を不変にしている．(10.1) により $\varepsilon_r=\varepsilon_{-r}$ が成り立つ．$\varepsilon_r=1$ とすれば ρ 不変な元の全体は明らかに $SL(2, F_0)$ と同形である．$SL(2, F_0)$ はベキ単3角行列により生成されるから（II §2）$h_J(t) \in \langle x_J(u), x_{-J}(v)\rangle$ $(u, v \in F_0)$ となる．すなわち，$h_J(t)$ は Steinberg 群の元となり $h_J(t) \in H_1$ を得る．

$\varepsilon_r=-1$ の場合は ρ が体型自己同形と共役になることを証明しよう．G_r を (2, 2) 型の行列のつくる群と同一視して，行列

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

を A とおけば $\rho(M)=A\theta(M)A^{-1}$ となる．よって $\theta(\gamma)=-\gamma$ をみたす F の元 γ をとり(定理 II 6.2 の証明参照)

$$\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}$$

による共役写像を δ とおけば $\rho=\delta\theta\delta^{-1}$ となる．明らかに ρ 不変な元のつくる G_r の部分群は θ 不変な元のつくる部分群 $SL(2, F_0)$ と同形である．この場合も $h_J(t)$ $(t \in F_0)$ は H_1 に含まれている．

σ 軌道 J が $A_1{}^2$ 型（または $A_1{}^3$ 型）の場合 G_r と $G_{\sigma(r)}$ とは元別に可換である．すなわち $\langle G_r, G_{\sigma(r)}\rangle = G_r \times G_{\sigma(r)}$（または3因子）となり ρ は直積因子を交換する．したがって $\langle x_J(t), x_{-J}(s)\rangle$ は $SL(2, F)$ と同形になる．したがってこの場合も $h_J(t) \in G_1$ が成り立つ．

軌道 J が A_2 型の場合には §10.2 で証明したように

$$\langle x_J(t, u), x_{-J}(t', u')\rangle$$

はユニタリ群 $SU(h)$ と一致する．よってこの場合も $h_J(t) \in G_1$ を得る．

すべての場合に $h_J(t) \in H_1 = G_1 \cap H$ が証明されたので $H_1 = H_2$ となり定理

が成り立つ．□

前に (§8.3) H の元を重みの生成する格子 Γ_V の指標として表わした．特に G が普遍的ならば (8.8) により H は重み加群 Q の指標群と同形になる．そこで定理 11.16 を指標を用いて書き直しておこう．根系の自己同形 τ は自然に $h_r \longmapsto h_{\tau(r)}$ と $\mathcal{H}$ の自己同形を定義する．重み加群 Q の定義 (4.25) により Q の自己同形 τ があって，$q\in Q, h_r\in\mathcal{H}$ について

$$\tau(q)(h_{\tau(r)})=q(h_r)$$

が成り立つ．明らかに，この自己同形 τ は P の上ではもとの τ と一致している．さて任意の指標 $\chi: Q\to F^{\#}$ に対して $\rho(\chi)$ を

$$\rho(\chi)(\tau q)=\theta(\chi(q)) \qquad (q\in Q)$$

と定義する．$\chi=\rho(\chi)$ をみたす Q の指標 χ を**自己共役**ということにしよう．この時，次の命題が成り立つ．

(11.17)　普遍的 Chevalley 群 G において H の元 y に対応する指標を χ_y とおく (§8.3参照)．この時 $\rho(\chi_y)=\chi_{\rho(y)}$ が成り立つ．G から定義された Steinberg 群 G_1 において H_1 は Q の自己共役指標全体のつくる群と同形である．

証明　§8.1 の記号を用いる．基本系 $\{r_1,\cdots,r_l\}$ の各元 r_i に対応して H の生成元 $h_i(t)$ が定まる．$\tau(r_i)=r_{\tau(i)}$ により置換 τ を定義する．H の元 y は $y=\prod h_i(t_i)$ と一意的に表わすことができる (8.4)．よって

$$\rho(y)=\prod h_{\tau(i)}(\theta(t_i))$$

となる (11.3)．さて §8.3 の定義により y に対応する指標は $q_i\longmapsto t_i$ をみたす元である．また $\chi_{\rho(y)}$ は $q_{\tau(i)}\longmapsto\theta(t_i)$ をみたすから

$$\chi_{\rho(y)}(\tau(q_i))=\chi_{\rho(y)}(q_{\tau(i)})=\theta(\chi_y(q_i))$$

がすべての i について成り立つ．よって $\rho(\chi_y)$ の定義から $\chi_{\rho(y)}=\rho(\chi_y)$ を得る．残りの命題はいまや明らかである．□

4. $G_1/Z(G_1)$ の単純性　単純性の証明は定理 9.3 の証明と同様である．まず次の補題を証明しよう．

(11.18)　G を普遍 Chevalley 群，G_1 を G から構成された Steinberg 群とする．4 元体上の A_2 型の群を除けば G_1 の交換子群は G_1 と一致する．

証明　前節のように H の元に重み加群 Q の指標を対応させる．H_1 の元 y

に対応する指標を χ とおけば χ は自己共役で

$$[y, x_r(u)] = x_r((\chi(r)-1)u)$$

が成り立つ．G_1 の生成元は Π の σ 軌道 J に関する $x_J(t), x_J(t,u)$ などの形をしている (11.11)．そこで場合を分けておのおのの場合に $x_J(t)$ などが交換子群の元となることを証明しよう．まず $|F_0|>2$ と仮定する．

Q の基 $\{q_i\}$ をとり根 r_j を $\{q_i\}$ の一次結合として表わす．その係数がつくる行列は根系 Δ の Cartan 行列と一致する (8.11)．自己共役指標 χ は基の元に対して $\theta(\chi(q_i))=\chi(q_{\tau(i)})$ をみたす以外 $\chi(q_i)$ の値は任意にとることができる．

まず $J=\{r\}$ と仮定する．この場合 $x_J(t)=x_r(t)$ だから $\chi(r)\neq 1$ をみたす自己共役指標が存在すれば $x_r(t)$ は交換子となる．さて $\Delta=A_l$ の時 $J=\{r\}$ となるのは $l=2k-1$ が奇数で $r=-q_{k-1}+2q_k-q_{k+1}$ の場合である．いますべての自己共役指標 χ について $\chi(r)=1$ と仮定すれば，任意の $F_0{}^{\#}$ の元 a と任意の $\alpha\in F^{\#}$ について $\alpha\theta(\alpha)=a^2=1$ が成り立つ．よって F_0 は2元体となり（II (3.6)参照）仮定 $|F_0|>2$ に矛盾する．$\Delta=D_l$ の場合は§3.4の記号で $r=r_i$ $(i<l-1)$ となる．よって r を $\{q_i\}$ の一次結合として表わした時，少なくとも一つの添数 j について q_j の係数は -1 かつ $j\leqq l-2$ となる．よって $|F_0|>2$ の時 $\chi(r)\neq 1$ をみたす自己共役指標がある．$\Delta=D_4$ の場合 $\sigma^2=1$ ならば上と同様，$\sigma^3=1$ の時は $r=r_2$ で $r=-q_1+2q_2-q_3-q_4$ となる．よって $\chi(q_1)=\chi(q_2)=t\in F_0{}^{\#}$ とおけば $\chi(r)=-t$ となる．すなわちこの場合も命題が成り立つ．$\Delta=E_6$ の場合は前の記号 (§3.7) で $r=r_2=2q_2-q_4$ または $r=r=-q_2-q_3+2q_4-q_5$ だから $|F_0|>2$ ならば $\chi(r)\neq 1$ をみたす自己共役指標 χ がある．

次に $\sigma(r)\neq r$ と仮定する．この時，例外の場合，すなわち $\Delta=A_2$ で $|F_0|=2$ の場合を除けば $\chi(r)\neq 1$ をみたす自己共役指標 χ が存在することを証明しよう．そこで任意の自己共役指標 χ に対して $\chi(r)=1$ が成り立つと仮定する．まず $r=2q_i-q_j$ と書けているとすれば $\chi(r)=\chi(q_i)^2\chi(q_j)^{-1}$ となる．したがって $\chi(q_j)$ は $\chi(q_i)$ により定まる．よって $q_j=\tau(q_i)$ となる．Cartan 行列の表から $\Delta=A_2$ 型であることがわかる．さらに任意の $a\in F^{\#}$ について $\theta(a)=a^2$ が成り立つ．よって F は4元体で例外の場合となる．次に $r=2q_i-q_j$ と書け

ていないと仮定する．Cartan 行列の表から

$$r=-q_u+2q_v-q_w, \quad \tau(q_u)\neq q_v, q_w$$

と書けていることがわかる．しかしこれは $\chi(r)=1$，すなわち $\chi(q_u)$ は χ が q_v, q_w でとる値によって定められるという仮定に矛盾する．よって例外の場合を除けば $\chi(r)\neq 1$ をみたす自己共役指標が存在する．

さて σ 軌道 J が $A_1{}^2$ 型（または $A_1{}^3$ 型）とする．$r\in J$ を一つ定めた上で前のように $x_J(t)$ を定義する(11.11)．$\chi(r)\neq 1$ をみたす自己共役指標 χ をとり，χ に対応する H_1 の元を y とおく．この時

$$[y, x_J(u)]=x_J((\chi(r)-1)u)$$

が成り立つ．よって任意の $t\in F^{\#}$ について $x_J(t)$ は G_1 の交換子となる．

軌道 J が A_2 型とする．この時も同様に

$$[y, x_J(u, v)]=x_J((\chi(r)-1)u, v')$$

を得る．そこで例外の場合を除けば，任意の $t\in F^{\#}$ に対して $x_J(t, v)$ が交換子となる元 v が少なくとも一つ存在する．ところで (11.11) により

$$[x_J(t_1, u_1), x_J(t_2, u_2)]=x_J(0, \varepsilon(\theta(t_1)t_2-t_1\theta(t_2)))$$

を得る．ここで $\varepsilon=\varepsilon_r N_{r,\tau(r)}=\pm 1$ である．いま $\gamma=-\theta(\gamma)$ をみたす F の元 γ を任意に選べば $\gamma=\varepsilon(\theta(t_1)t_2-t_1\theta(t_2))$ をみたす t_1, t_2 の存在することが容易に証明される．よって $x_J(0,\gamma)$ は交換子である．$t\in F^{\#}$ を定めた時，任意の u について $x_J(t,u)=x_J(t,v)x_J(0,\gamma)$ をみたす元 γ が存在するから $x_J(t,u)$ は G_1 の交換子群の元である．

以上で $|F_0|>2$ の場合に (11.18) の成り立つことが証明された．そこで以後では $|F_0|=2$ と仮定する．例外の場合を除けば $J=\{r\}$ の時 $x_J(t)$ が交換子群に含まれていることを証明すればよい．

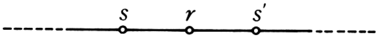
$\varDelta$ に対応する Dynkin の図形で r と s とが結ばれていてしかも $\tau(s)=s$ となっている場合を考えよう．この時 r と s とが生成する根系は A_2 型である．また Weyl 群の元 w_r, w_s は W_1 に含まれている(11.4)．そこで

$$[x_r(t), x_s(u)]=x_{r+s}(N_{r,s}tu) \qquad (N_{r,s}=\pm 1)$$

および $w_s(r+s)=r$ が成り立つから G_1 の中で $x_J(v)$ は交換子となる．よって E_6 および D_l $(\sigma^2=1)$ の場合 (11.18) が成り立つ．D_4 で $\sigma^3=1$ の場合，σ 軌道は $J_1=\{r_1, r_3, r_4\}$ および $J_2=\{r_2\}$ である．W_1 は G_2 型で，J_1 に対応す

る元が短い根，J_2 に対応するのが長い根である．定理 9.3 の証明と同様に長い根に対応する群が交換子群に含まれることがわかる．

最後に A_l 型の場合を考えよう．この時 $J=\{r\}$ とすれば



で $s'=\sigma(s)$ となる．$\{s,r,s'\}$ は A_3 型の根系をつくり，正根は $s,r,s',s+r,r+s',s+r+s'$ である．W_1 に属する元 $w_1=w_sw_{s'}$ により $r+s+s'$ と r とが入れ換わる．さて F の標数が 2 で $N_{r,s}$ などが 1 だから

$$[x_r(1),x_s(u)x_{s'}(u')]=x_{r+s}(u)x_{r+s'}(u')x_{r+s+s'}(uu')$$

が成り立つ．$I=\{s,s'\}$ とおけば $x_{r+s}(u)x_{r+s'}(u')$ は $x_I(u)$ と共役だから交換子群に含まれている．したがって $x_{r+s+s'}(uu')$ は G_1 の交換子群の元となる．$x_J(1)$ は $x_{r+s+s'}(1)$ と G_1 の中で共役だから $x_J(1)$ も G_1 の交換子群の元である．

G_1 の生成元はいずれの場合も G_1 の交換子群に含まれている（例外の場合は除く）．よって G_1 の交換子群は一つの例外を除いて G_1 に一致する．□

定理 11.19　普遍 Chevalley 群から定義される Steinberg 群を G_1 としその中心を Z とおく．4 元体上の A_2 型の場合を除けば G_1/Z は単純である．

証明　定理 11.14 により (G_1,B_1,N_1,S_1) は Tits 系をつくる．B_1 に含まれる G_1 の正規部分群のうち最大のものを Z_1 とおき $Z_1=Z(G_1)$ を証明しよう．根系のすべての根の符号を変える元を w_0 とすれば $w_0\in G_1$ となる．よって $Z_1\subset B_1\cap w_0B_1w_0^{-1}\subset B_1\cap V_1H_1=H_1$ が成り立つ．定理 9.3 の証明と同様に $Z_1\subset Z(G_1)$ となる．定理 7.19 (vi) により $Z(G_1)\subset B_1$ が成り立つので $Z_1=Z(G_1)=Z$ を得る．

さて $\overline{G}=G_1/Z$ とおき $\overline{B},\overline{N},\overline{S}$ をそれぞれ B_1,N_1,S_1 の像とすれば Z が H_1 に含まれているから $(\overline{G},\overline{B},\overline{N},\overline{S})$ も Tits 系をつくる．ここでこの Tits 系が (9.1) の条件をみたしていることを証明しよう．

例外の場合を除けば G_1 の交換子群は G_1 と一致する (11.18)．$\overline{G}$ は G_1 の準同形像だから $\overline{G}'=\overline{G}$ となり条件(1)が成り立つ(『群論』下 p.410 参照)．

条件(2)が成り立つことは明らかである．また $\overline{G}$ の定義により $\overline{B}$ に含まれている $\overline{G}$ の正規部分群は $\{1\}$ しかない(同形対応定理，『群論』上 p.38)．よっ

て条件(3)が成り立つ．$\overline{G}$ の Weyl 群は G_1 のものと同形だから条件(4)も成り立つ．よって (9.1) により例外の場合は除いて $\overline{G}$ は単純である． ▯

5. 普遍型 Steinberg 群の中心

(11.20) 普遍 Chevalley 群を G，それから構成された Steinberg 群を G_1 とする．この時 $Z(G_1)=G_1\cap Z(G)$ が成り立つ．

証明 前定理の証明において $Z(G_1)\subset H_1$ の成り立つことが示されている．そこで $Z(G_1)$ の元 y に対応する指標を χ とおけば (§8.3参照) (11.18) の証明からわかるように

$$yx_J(t)y^{-1}=x_J(\chi(r)t)$$
$$yx_J(t,u)y^{-1}=x_J(\chi(r)t,v)$$

($r\in J$, v は t,u,y により定まる元) が成り立つ．さて $y\in Z(G_1)$ だから，任意の r について $\chi(r)=1$ となる．すなわち，y は G の元として，G の中心に含まれている．よって $Z(G_1)=G_1\cap Z(G)$ が成り立つ． ▯

系 随伴的 Chevalley 群は $G_1/Z(G_1)$ という形の Steinberg 群を含む．

証明 普遍 Chevalley 群を G とすれば随伴的 Chevalley 群は $G/Z(G)$ と同形である (定理 8.6 および 9.3)．よって G_1 から $G/Z(G)$ の中への自然準同形による像は $G_1Z(G)/Z(G)\cong G_1/G_1\cap Z(G)$ である．(11.20) によりこの式の右辺は $G_1/Z(G_1)$ と一致する． ▯

定理 11.21 普遍 Chevalley 群から定義された Steinberg 群を G_1 とする．G_1 の中心 $Z(G_1)$ は有限巡回群でその位数 d は次の通りである．

A_l 型　$\alpha\theta(\alpha)=1$ をみたす $l+1$ 乗根の数が d と一致する．F_0 が q 元体の場合は $d=(l+1,q+1)$ となる．

D_l 型 ($\sigma^2=1$)　体 F の標数が 2 ならば $d=1$，標数が 2 でない時 l が奇数で 1 の原始 4 乗根が $F-F_0$ に含まれていれば $d=4$，それ以外の場合は $d=2$ である．F_0 が q 元体ならば $d=(4,q^l+1)$ となる．

D_4 型 ($\sigma^3=1$)　$Z(G_1)=\{1\}$，すなわち $d=1$ である．

E_6 型　1 の原始 3 乗根が $F-F_0$ に含まれている場合に限り $d=3$，その他の場合は $d=1$ である．$|F_0|=q$ ならば $d=(3,q+1)$.

証明 G_1 の中心元 y に対応する指標を χ とおく．χ は自己共役で，任意の根 r について $\chi(r)=1$ をみたす．そのような指標は次のようにして求めるこ

とができる．

根 r_i を基 $\{q_i\}$ を用いて表わせば係数のつくる行列は Δ の Cartan 行列と一致する．指標は q_i における値で定まる．これらの値は $\chi(r)=1$ をみたさねばならない．これから各型に応じて χ に対する制限が得られ，定理が証明される．それを実行してみよう．

A_l 型　$r_1=2q_1-q_2, r_2=-q_1+2q_2-q_3, \cdots$ だから $\chi(q_1)=t$ とおけば $\chi(q_2)=t^2, \chi(q_3)=t^3, \cdots, \chi(q_l)=t^l$ と一意的に定まる．最後に

$$r_l=-q_{l-1}+2q_l \Longrightarrow t^{l-1}=t^{2l} \Longrightarrow t^{l+1}=1$$

を得る．しかも χ は自己共役だから $\chi(q_l)=\theta(\chi(q_1))$ すなわち $\theta(t)=t^l, \theta(t)=t^{-1}$ が成り立たなくてはならない．逆に $t\theta(t)=1$ をみたす1の $l+1$ 乗根を t とすれば $\chi(q_i)=t^i$ は自己共役指標となり $\chi(r)=1$ が成り立つ．よって A_l 型の Steinberg 群について定理が成り立つ．

D_l 型 $(\sigma^2=1)$ の場合 $\chi(q_1)=t, \chi(q_{l-1})=u, \chi(q_l)=v$ とおけば A_l 型の場合と同様に $\chi(q_i)=t^i$ $(i\leqq l-2)$ および $uv=t^{l-1}, u^2=v^2=t^{l-2}$ を得る．(D_l 型の Cartan 行列を参照）上式より $t^2=1$ を得る．よって F の標数が2ならば $d=1$ である．F の標数が2でないと仮定する．l が偶数ならば

$$u^2=v^2=1, v=\theta(u) \Longrightarrow u=v, t=1$$

を得る．よって $d=2$ となる．l が奇数の場合 $t=-1$ が可能になるのは，1の原始4乗根が $F-F_0$ に含まれている場合で，この時は $d=4$ となる．

D_4 型 $(\sigma^3=1)$ の場合は上の記号で t, u, v は共役である．よって $uv=t$ より $t=u=v=1$ となり $d=1$ を得る．

E_6 型　$\chi(q_1)=t, \chi(q_2)=s$ とおけば Cartan 行列の形から

$$\chi(q_3)=t^2, \quad \chi(q_4)=s^2=t^3, \quad \chi(q_5)=st, \quad \chi(q_6)=t^2$$

さらに $t^4=st$ となる．よって $t^3=s=1$ を得る．χ は自己共役だから

$$\theta(t)=t^2$$

が成り立つ．よって $F-F_0$ が原始3乗根を含んでいる時かつその時に限り，中心の位数は3となる．□

6. 有限単純 Steinberg 群の位数　普遍 Chevalley 群を G, G に対応する根系を Δ, その正系を Δ^+ とし $U=\langle x_r(t)\,|\,r\in\Delta^+, t\in F\rangle$ とおく．G から構成される Steinberg 群を G_1 とする．この節では F が有限体の場合に G_1 の

位数を計算しよう．そのため

$$q=|F_0|$$

とおく．ここで F_0 は θ の不変体である．

(11.22) 上の記号の下で $|U_1|=q^N, N=|\varDelta^+|$, が成り立つ．

証明 (11.1)により τ は $\varDelta^+$ を不変にする．まず Π 上の σ 軌道に A_2 型はないと仮定する．この時 $\varDelta^+$ の τ 軌道の一つを J とすれば W_1 の元 w があって $w(J)$ が Π の σ 軌道となることを証明しよう．いま $s\in J$ とすれば(11.10)により W_1 の元 w と Π の σ 軌道 I があって $w(s)\in I^+$ となる．仮定により I は A_2 型でないから I^+ は I と一致し，$w(s)\in I$ となる．さて

$$w(\tau(s))=\tau(w(s))=\sigma(w(s))\in I$$

となるから $w(J)\subset I$ が成り立つ．よって $w(J)=I$ となる．

A_2 型の軌道がある場合でも I が A_2 型でなければ $w(J)=I$ となる．I が A_2 型の場合は J に対応して $\varDelta^+$ の τ 軌道 J' が定まり $w(J\cup J')=I^+$ となる．この時 $J^+=J\cup J'$ とおく．I が A_2 型でない場合は $J^+=J$ とおく．以上のことから $\varDelta^+$ は $\{J^+\}$ の直和に分解する．さて

$$U(J^+)=\langle x_r(t)\,|\,r\in J^+, t\in F\rangle$$

とおけば $U(J^+)$ は G_1 の中で $U(I^+)$ と共役で，$U_1(J^+)=G_1\cap U(J^+)$ とおけばそれは $U_1(I^+)$ と同形である．特に $U_1(J^+)$ の位数は q^n $(n=|J^+|)$ となる．$U_1=\prod U_1(J^+)$ が成り立つから $|U_1|=q^N$ となる． □

定理 11.23 上命題と同じ記号の下で G_i の位数は

$$|G_1|=q^N\prod_i(q-\varepsilon_i)\sum_{w\in W_1}q^{l(w)}$$

となる．ここで $\{\varepsilon_1,\cdots,\varepsilon_l\}$ は E 上の作用 τ の固有値の集合である．

証明 (11.13) により G_1 の元は一意的に

$$unv \qquad (u\in U_1, n\in N_1, v\in U_1\cap U_w^-, w\in W_1)$$

と表わすことができる．各 $w\in W_1$ について U_w^- は W_1 不変であるから

$$U_1\cap U_w^-=\prod U_1(J^+)$$

と分解する．よって $|U_1\cap U_w^-|=q^{n(w)}$ ($n(w)$ は w により符号を変える正根の数) が成り立つ．定理 1.13 により $n(w)=l(w)$ となるから次式を得る．

$$|G_1|=|U_1||H_1|\sum q^{l(w)}.$$

定理 11.16 により H_1 の元は $\prod h_J(t_J)$ という形に一意的に書ける．ここで

JはΠのσ軌道全体を動く．$|J|=1$ の場合は $t_J \in F_0^{\#}$ で $q-1$ 個の可能な値をとる．$|J|>1$ の場合t_Jは$F^{\#}$の任意の元でよいから $|J|=2, 3$ に応じてそれぞれ q^2-1 または q^3-1 個可能な値がある．よって

$$|H_1|=\prod_{i=1}^{l}(q-\varepsilon_i)$$

となる $(q^3-1=(q-1)(q-\omega)(q-\omega^2),\ \omega^3=1)$． ▯

系　単純 Steinberg 群の位数は

$$(1/d)q^N\prod(q-\varepsilon_i)\sum q^{l(w)}$$

である．ここでdは $Z(G_1)$ の位数で定理11.21により与えられる． ▯

補足　Steinberg 群の位数は次のように書くことができる．

E_6型　$q^{36}(q^2-1)(q^5+1)(q^6-1)(q^8-1)(q^9+1)(q^{12}-1)$

D_4型 $(\sigma^3=1)$　$q^{12}(q^2-1)(q^6-1)(q^8+q^4+1)$ ▯

注意　定理11.19および(11.18)における例外の場合は，真に例外でG_1は位数72の可解群となる． ▯

§12　その他の Lie 型単純群

1. 例外グラフ型自己同形　複素単純 Lie 代数に対応する Dynkin の図形の表を見ると§10において考察した場合の外に対称性をもつ図形が三つある．すなわち B_2, F_4, G_2 型の場合，対称 $\sigma\neq 1$ が存在する．しかしA_l型などとちがって根rが短い根であればσrは長い根，rが長い根であればσrは短い根となっている．基本系Πを $\{r_1, \cdots, r_l\}$ とおけば σr_i と σr_j の間の角はr_iとr_jとの間の角と一致している．

§2において根系Δから $\Delta'=\{h_r\}$ を定義した．その時注意したようにΔ'はΔの双対根系である．いま $h_i=h_{r_i}$ とおけば $\{h_i\}$ がΔ'の基本系の一つとなり，h_iとh_jとの間の角は，r_iとr_jとの間の角と一致する．そしてr_iが短い根の時h_iはΔ'における長い根，r_jが長い根ならばh_jは短い根となっている．$\Delta=B_2, F_4, G_2$ の場合Δ'とΔは同形である．実際その同形写像が

$$\sum n_i h_i \longmapsto \sum n_i \sigma r_i$$

によって与えられる．そこでσを拡張してΔからΔの上への全単射σを定義することができる．任意の $r\in\Delta$ に対して $\sigma(r)$ は

$$h_r=\sum n_i h_i \Longrightarrow \sigma(r)=\sum n_i\sigma(r_i)$$

と定義される．たとえば $\Delta=B_2$ 型の場合 (1.4) の記号に従い $\Pi=\{r, s\}$ とし r が短い根とすれば，図形の対称は $\sigma: r\leftrightarrow s$ で与えられる．さて

$$h_r=2b_r, \quad h_s=b_s$$

だから（ここで$(r,r)=1$ と長さの単位を定めた）$b_{r+s}=b_r+b_s$ より

$$h_{r+s}=2b_{r+s}=h_r+2h_s, \qquad h_{2r+s}=b_{2r+s}=h_r+h_s$$

を得る．したがって

$$\sigma(r+s)=2r+s, \qquad \sigma(2r+s)=r+s$$

となる．すなわち B_2 型の根系において r と s との間の角の2等分線に関する対称により根 t を含む半直線が $\sigma(t)$ を含む半直線に移される．G_2 型の場合も同様で r と s との間の角の2等分線に関する対称が σ を表現することがわかる．

根が生成する Euclid 空間を E とおく．上述のように図形の対称を根系の全単射 σ に拡張できるが σ は明らかに E の等長写像ではない．しかし B_2 型または F_4 型の場合

$$\tau(r)=(1/\sqrt{2})\sigma(r) \qquad (r\text{ が短い根})$$
$$\tau(r)=\sqrt{2}\,\sigma(r) \qquad (r\text{ が長い根})$$

とおいて写像 τ を定義すれば，τ は E の等長写像に拡張できる．G_2 型の場合には係数を $1/\sqrt{3}$ または $\sqrt{3}$ と変えればよい．以下 B_2, F_4 型の場合，標数2の有限体の上で普遍 Chevalley 群が例外グラフ型自己同形をもつことを証明しよう．G_2 型の場合は標数3の有限体上で同様の結果が成り立つ．

定理 12.1 標数2の有限体 F 上で定義された B_2 型または F_4 型の普遍的 Chevalley 群を G とおく．任意の根 r について $\lambda(r)$ を

$$\lambda(r)=1 \quad (r\text{ が短い根}), \qquad \lambda(r)=2 \quad (r\text{ が長い根})$$

と定義する．この時，G は任意の $r\in\Delta$ および $t\in F$ について

$$\gamma(x_r(t))=x_{\sigma(r)}(t^{\lambda(\sigma(r))})$$

をみたす自己同形 γ をもっている．

証明 (10.1)の証明と同様 $\{x_{\sigma(r)}(t^{\lambda(\sigma(r))})\}$ が定理 8.6 の証明に現われる基本関係をみたすことを示せばよい．$\sigma(r)$ が短い根の場合に関係 (A) が成り立つことは明らかである．$\sigma(r)$ が長い根の場合は $\lambda(\sigma(r))=2$ である．しかし体 F の標数が2だから $(t_1+t_2)^2=t_1^2+t_2^2$ が成り立ち，この場合も関係 (A) が成

り立つ.

関係(B)を証明するため, $\{r, s\}$ を一次独立な根とする. まず $r+s$ が根でないと仮定する. この時 $X_{\sigma(r)}$ と $X_{\sigma(s)}$ とが元別に可換であることを証明しなくてはならない. これは $\sigma(r)+\sigma(s)$ が根でなければ明らかである. そこで $\sigma(r)+\sigma(s)$ が根であると仮定しよう. 2次元の根系を調べてみれば ((1.4)参照) これは $\sigma(r), \sigma(s)$ が共に短い根で B_2 型の根系を生成する場合である. ところで $[x_{\sigma(r)}(t), x_{\sigma(s)}(u)]=x_{\sigma(r)+\sigma(s)}(Ntu)$ において $N=N_{\sigma(r),\sigma(s)}$ は ± 2 に等しい (2.6). 体 F の標数が2だから, 上の交換子は1となり, この場合も $X_{\sigma(r)}$ と $X_{\sigma(s)}$ とは元別に可換である.

次に $r+s$ が根になると仮定しよう. この場合 r と s との間の角は $90°, 120°$ または $145°$ である. $90°$ の場合は上と同様に関係 (B) の成り立つことがわかる. 角が $120°$ の場合は r と s とは同じ長さで $N_{r,s}=\pm 1$ となる. また

$$\lambda(\sigma(r))=\lambda(\sigma(s))=\lambda(\sigma(r)+\sigma(s))$$

が成り立つ. そこで $\lambda=\lambda(\sigma(r))$ とおけば

$$[x_{\sigma(r)}(t^{\lambda}), x_{\sigma(s)}(u^{\lambda})]=x_{\sigma(r)+\sigma(s)}(t^{\lambda}u^{\lambda})$$

となる. 一方, $\sigma(r+s)=\sigma(r)+\sigma(s)$ であることが証明されるので関係 (B) が成り立つ. r と s との間の角が $135°$ の時, 短い根の方を r とすれば

$$[x_{\sigma(r)}(t^2), x_{\sigma(s)}(u)]=x_{\sigma(r+s)}((tu)^2)x_{\sigma(2r+s)}(t^2u)$$

が成り立つことを証明すればよい. 定理 7.1 により上式の左辺は

$$x_{\sigma(r)+\sigma(s)}(t^2u)x_{\sigma(r)+2\sigma(s)}(u^2t^2)$$

に等しい. ところで $\sigma(r+s)=\sigma(r)+2\sigma(s), \sigma(2r+s)=\sigma(r)+\sigma(s)$ となるから上式が成り立ち, 関係 (B) が証明される. r が長い根でも同様である.

定義から $\omega_r(t)$ に対応する元は $\omega_{\sigma(r)}(t^{\lambda(\sigma(r))})$ となる. $h_r(t)$ についても同様である. E の等長写像 τ により $\tau(r)$ は $\sigma(r)$ と同一方向にむかうベクトルだから $\tau w_r \tau^{-1}=w_{\tau(r)}=w_{\sigma(r)}$ および $\sigma(w_r(s))=w_{\sigma(r)}(\sigma(s))$ を得る. よって(7.6) (i) に対応する式が成り立つ. 体 F の標数が2だから (7.6)(ii) も成り立つ ($c(r, s)=\pm 1=1$). 容易に

$$n(s, r)\lambda(\sigma(s))=\lambda(\sigma(r))n(\sigma(s), \sigma(r))$$

となることが確かめられるので関係 (C) が成り立つ.

関係 (D) が成り立つことは明らかである. よって

$$\gamma(x_r(t))=x_{\sigma(r)}(t^{\lambda(\sigma(r))})$$

は G から G の中への準同形を与える．明らかに $\gamma^2(x_r(t))=x_r(t^2)$ となる．係数体 F が有限ならば（F は完全体で）写像 $t\longmapsto t^2$ は全単射となる．よって γ も全単射で G の自己同形となる． ▯

G_2 型の群の例外グラフ型自己同形を構成することは定理 12.1 と同様であるが，符号を一々決めなくてはならないのでもっと複雑になる．Ree [2*] を参照されたい．

2. 鈴木群，Ree 群，Tits 群　標数 2 の有限体 F が $\theta^2(t^2)=t$ をみたす自己同形 θ をもつと仮定する．この時 B_2 型，F_4 型の普遍 Chevalley 群は

$$\rho(x_r(t))=x_{\sigma(r)}(\theta(t)^{\lambda(\sigma(r))})$$

により定義される自己同形 ρ をもつ．定義から $\rho^2=1$ となる．σ は基本系 Π を不変にするから，ρ は部分群 U, V を不変にする．そこで

$$U_1=\{u\,|\,u\in U,\,\rho(u)=u\}$$

とおき，同様に V_1 を V の ρ 不変元の全体と定義する．そして

$$G_1=\langle U_1,\,V_1\rangle$$

とおく．この時 G_1 について §11 で Steinberg 群について述べたことと同様な結果が成り立つ．特に $|F|>2$ の場合単純群が得られる．証明は §11 と同様だから変更しなければならない点だけを述べ細部は省略する．

一般に $\rho(\omega_r)=\omega_{\sigma(r)}$ が成り立つ．そこで ρ が引きおこす Weyl 群の自己同形を §11 のように同じ文字 ρ で表わすことにする．この時

$$\rho(w)=\tau w\tau^{-1}\qquad(w\in W)$$

が成り立つ．さて Π 上の σ 軌道 J をとり J に含まれる短い根を r とおけば $\sigma(r)$ は長い根で $J=\{r,\sigma(r)\}$ となる．J の生成する正根の集合は

$$J^+=\{r,\sigma(r)\},\quad J^+=\{r,\sigma(r),r+\sigma(r),2r+\sigma(r)\}$$

のいずれかである．§11 と全く同様に (11.7) および (11.8) が成り立つ．また (11.9) の前半も同様に証明される．ρ 不変な W の元全体のつくる群を W_1 とおけば，B_2 型の時 W_1 は位数 2 の巡回群である．

(12.2)　F_4 型の場合 W_1 は位数 16 の 2 面体群である．

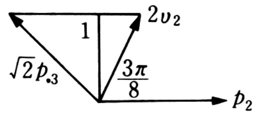
証明　F_4 型の根系を §3.8 のように番号をつけ $\{p_1,p_2,p_3,p_4\}$ とおく．この時 p_1,p_2 が長い根で p_3,p_4 が短い根である．そこで

$$\tau(p_1)=\sqrt{2}\,p_4,\quad \tau(p_2)=\sqrt{2}\,p_3$$

となる．二つの σ 軌道に対応する W_1 の生成元は（(11.9)参照）

$$v_1=(p_1+\sqrt{2}\,p_4)/2,\quad v_2=(p_2+\sqrt{2}\,p_3)/2$$

に関する対称変換である．よって W_1 は 2 面体群でその位数は v_1 と v_2 との間の角 φ により定められる．p_3 の長さを 1 にとれば p_1 の長さは $\sqrt{2}$，v_1 の長さは 1，　v_2 の長さは $1/(2\cos(\pi/8))$ となる(次図参照)．



さて $(p_1, p_2)=-1, (p_3, p_4)=-1/2$ だから

$$\cos\varphi=2\cos(\pi/8)(v_1, v_2)=-\cos(\pi/8)$$

となる．したがって $\varphi=7\pi/8$ を得るから W_1 の位数は 16 である．　□

σ 軌道 J が $A_1{}^2$ 型の場合 $U(J)$ の構造は簡単で $\{x_r(t)x_{\sigma(r)}(t^2)\}$ となる．しかし J が B_2 型の場合は次の様になる．$\sigma(r)=s$ とおいて

$$x=x_r(t_1)x_s(t_2)x_{r+s}(t_3)x_{2r+s}(t_4)$$

が ρ 不変となるための条件を求めよう．定理 7.3 を用いれば

$$t_1=\theta(t_2),\quad t_3=\theta(t_1{}^2t_2+t_4)$$

を得る．すなわち $U_1(J)$ の元は $t=t_2, u=\theta(t_4)$ を用いて

$$x_r(\theta(t))x_s(t)x_{r+s}(t\theta(t)+u)x_{2r+s}(\theta(u^2))$$

と表わすことができる．さて $B_2=C_2$ だから B_2 型の普遍 Chevalley 群は 4 次元の斜交群 $Sp(4, F)$ である(§8.2 節末の注意 1)．§3.3 の記号を用い

$$r=e_1-e_2,\quad s=2e_2,\quad r+s=e_1+e_2,\quad 2r+s=2e_1$$

と正根を定めれば生成元 $x_r(t)$ などを (4, 4) 型行列で表わすことができる．

$$x_r(t)=I+tu_{12},\quad x_s(t)=I+te_{24}$$

$$x_{r+s}(t)=I+ts_{12},\quad x_{2r+s}(t)=I+te_{13}$$

であるから上に与えた $U_1(J)$ の元を $x(t, u)$ とおけば $x(t, u)$ は

$$\begin{pmatrix} 1 & \theta(t) & \xi & u \\ & 1 & \eta & t \\ & & 1 & \\ & & \theta(t) & 1 \end{pmatrix}\qquad \begin{aligned} \xi&=\theta(u^2)+t\theta(t^2)+u\theta(t) \\ \eta&=t\theta(t)+u \end{aligned}$$

(空いている場所は 0）という斜交群の元に対応する．これから

$$x(t,u)x(t',u')=x(t+t',u+u'+\theta(t)t')$$

が成り立つ．すなわち (11.11) の類似が成り立つ．(11.12) および (11.13) がそのまま成り立つので定理 11.14 が成り立つ．よって G_1 は Tits 系をもっている．部分群 H に含まれる ρ 不変元は (11.15) と同様に $\prod h_J(t_J)$ と一意的に表わすことができる．ここで r を J に含まれる短い根とすれば

$$h_J(t)=h_r(t)h_{\sigma(r)}(\theta(t^2))$$

である．定理 11.16 も成り立つ．J が $A_1{}^2$ 型の場合は前と同様である．J が B_2 型の場合 $Sp(4,F)$ の中で $\omega_r(t)$ および $\omega_s(u)$ に対応する行列は

$$\begin{pmatrix} & t & & \\ t^{-1} & & & \\ & & & t^{-1} \\ & & t & \end{pmatrix},\quad \begin{pmatrix} 1 & & & \\ & & & u \\ & & 1 & \\ & u^{-1} & & \end{pmatrix}$$

となる．$w_0(J)$ に対応する元は $(\omega_r\omega_s)^2$ であるから行列

$$\begin{pmatrix} & & y & \\ & & & z \\ y^{-1} & & & \\ & z^{-1} & & \end{pmatrix}$$

が W_1 の生成元に対応する．この行列で表わされる元を $n(y,z)$ とおく．V の元 $v=x_{-(r+s)}(\theta(t))x_{-(2r+s)}(t)$ をとる．明らかに v は ρ 不変だからその標準形は $v=x(x,u)n(y,z)x(x',u')$ となり $n(y,z)\in G_1$ が成り立つ (11.13)．この式を行列の式に書き直して，(2,2) 型の小行列に分けて書けば

$$\begin{pmatrix} I & 0 \\ T & I \end{pmatrix}=\begin{pmatrix} X & A \\ 0 & {}^tX \end{pmatrix}\begin{pmatrix} 0 & D \\ D^{-1} & 0 \end{pmatrix}\begin{pmatrix} X' & A' \\ 0 & {}^tX' \end{pmatrix}$$

となるから $T={}^tXD^{-1}X'$ を得る．すなわち，任意の $t\in F^*$ に対し

$$\begin{pmatrix} t & \theta(t) \\ \theta(t) & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ \theta(x) & 1 \end{pmatrix}\begin{pmatrix} y^{-1} & 0 \\ 0 & z^{-1} \end{pmatrix}\begin{pmatrix} 1 & \theta(x') \\ 0 & 1 \end{pmatrix}$$

が成り立つ．したがって $t=y^{-1},\theta(t)=y^{-1}\theta(x)=y^{-1}\theta(x')$ および

$$\theta(x)y^{-1}\theta(x')+z^{-1}=0$$

となる．すなわち，任意の t について $t'=\theta(t^2)t^{-1}$ とおけば $n(t,t')$ は G_1 の元

となる．特に $n(1,1)\in G_1$．よって $n(t,t')n(1,1)$ も G_1 の元である．行列の計算により(空所は 0)

$$\begin{pmatrix} & & t & \\ & & & t' \\ t^{-1} & & & \\ & t'^{-1} & & \end{pmatrix}\begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}=\begin{pmatrix} t & & & \\ & t' & & \\ & & t^{-1} & \\ & & & t'^{-1} \end{pmatrix}$$

となる．ところで $h_r(t), h_s(u)$ はそれぞれ

$$\begin{pmatrix} t & & & \\ & t^{-1} & & \\ & & t^{-1} & \\ & & & t \end{pmatrix},\ \begin{pmatrix} 1 & & & \\ & u & & \\ & & 1 & \\ & & & u^{-1} \end{pmatrix}$$

に対応している．したがって $n(t,t')n(1,1)=h_r(t)h_s(\theta(t^2))$ が成り立つ．これは σ 軌道 J が B_2 型の場合にも $h_J(t)\in G_1$ が成り立つこと，すなわち H_1 が H に含まれている ρ 不変元の全体と一致することを示している．よって定理 11.16 が成り立つ．

係数体 F が $|F|>2$ をみたす場合には G_1 は単純群になる．この証明も定理 11.19 の証明と同様である．標数 2 の体の上では B_2 型でも F_4 型でも普遍的な Chevalley 群の中心は $\{1\}$ だから $Z(G_1)$ も $\{1\}$ となる．

B_2 型の場合 G_1 は B_1 に関する剰余類の上の置換群として 2 重可移となっている．この群は，はじめ 2 重可移群の研究中に鈴木 [3*] により発見されたので鈴木群と呼ばれている．群 G_1 は斜交群 $Sp(4,F)$ の部分群として定義されたが，それが例外的自己同形による不変元の全体となることは小野 [1*]，Ree により独立に証明され，その類似として Ree[2*] が F_4 型の群を定義した．そのため F_4 型の群は Ree 群といわれている．B_2 型の群は係数体が 2 元体の時，位数 20 の可解群となる．F_4 型の場合 $|F|=2$ ならば単純群ではない．この場合には G_1 は指数 2 の正規部分群 T を含むこと，そして T は非可換単純群であることを Tits が証明した．T は Tits 群と呼ばれている．この群については Tits [1*] を参照されたい．

鈴木群，Ree 群の位数も §11.6 と同様の方法により求めることができる．結果だけ書いておこう．$q=|F|$ とおく．

B_2 型 $\quad q^2(q-1)(q^2+1)$

F_4 型 $\quad q^{12}(q-1)(q^3+1)(q^4-1)(q^6+1)$

Tits 群の位数は $q=2$ で F_4 型の式の半分となる．

注意 係数体 F は標数 2 で $\theta^2(t^2)=t$ をみたす自己同形をもっている．F は有限体だから $\theta(t)=t^r$ (r は 2 のベキ) となる．よって $|F|=2^n$ とおけば $2r^2=2^n$ が成り立つ．したがって n は奇数でなければならない． □

3. 標数 3 の Ree 群 標数 3 の有限体 F の上で G_2 型の普遍 Chevalley 群は例外グラフ型自己同形 γ をもっている．γ は

$$\gamma(x_r(t))=x_{\sigma(r)}(t^{\lambda(\sigma(r))})$$

をみたす．ここで $\lambda(r)$ は r が短い根の時 1，長い根の時 3 とする．標数 2 の場合と同様 F が $\theta^2(t^3)=t$ をみたす自己同形をもっていれば

$$\rho(x_r(t))=x_{\sigma(r)}(\theta(t)^{\lambda(\sigma(r))})$$

により定義される自己同形 ρ があり，ρ 不変元のつくる部分群が前と同様に定義される．$|F|=q=3^n$ とおけば，n は奇数で G_1 の位数は

$$q^3(q-1)(q^3+1)$$

となる．$q>3$ ならば G_1 は単純群，$q=3$ の時は G_1 は指数 2 の正規部分群を含んでいる．この指数 2 の部分群は $SL(2,8)$ と同形である．これらの事実の証明は前と同様であるが Ree [2*] を参照されたい．この群も Ree 群と呼ばれている．

第4章　散在単純群

§1　散在単純群の歴史

単純群の分類定理（I §1）において最後にまとめられている散在単純群は無限系列に属していない例外的な単純群で全部で26個ある．そのうち最も古くから知られている群は Mathieu によって百年以上前に発見された次数12の5重可移群 M_{12} と次数24の5重可移群 M_{24} である．Mathieu が発見したあとしばらくしてこれらの群は単純群であることが証明された．M_{24} の中で1点の安定化群，2点の安定化群，3点の安定化群はそれぞれ次数23の4重可移群，次数22の3重可移群，次数21の2重可移群となる．これらの群もすべて単純群となり M_{23}, M_{22} と表わされている．最後の次数21の2重可移群は4元体上の $PSL(3,4)$ が射影平面の点の上に作用している置換群と同形となる（II §2参照）．小さい Mathieu 群 M_{12} の場合，1点の安定化群は M_{11} と表わされる単純群であるが，2点の安定化群は位数720の群で指数2の正規部分群（交代群 A_6 と同形）を含んでいる．Mathieu 群が単純であることは永尾 [4]，大山 [5] に解説されている．本書では残念ながら各散在群についてその単純性を詳しく説明することはできないが，あとで Mathieu 群も含めて一応の証明を述べることにする．

Mathieu の5重可移群に関する論文が1860年頃発表されて以来百年もの間新しい散在単純群は発見されず影をひそめていた．1955年に Chevalley の論文が発表され Chevalley 群がはっきり定義されると，相ついで Steinberg 群，鈴木群，Ree 群，Tits 群が発見され，いわゆる Lie 型の単純群が全部現われた．これより先，有限群論の進展により有限単純群を研究しようという気運が高まっていた．そのもととなるのは次の Brauer-Fowler の定理である．

偶数位数の有限単純群を G とする．G に含まれている位数2の元 t について，その中心化群 $C_G(t)$ の構造が与えられていると仮定すれば，$C_G(t)$ によって定まる或る定数 N があって G の位数は N 以下となる．すなわち，$C_G(t)$ の

構造によって単純群Gはほとんど定まってしまう.（詳しいことは『群論』下,参照. 特に p. 510 および p. 759.）

この定理により単純群では位数2の元の中心化群が特に注目される. 前に述べた鈴木群の発見も $C_G(t)$ がベキ零となる単純群を決定しようという研究の中から導かれたものである. G_2型の Ree 群では位数2の元全体は一つの共役類をつくり, その1元tをとれば $C_G(t)=\langle t\rangle\times PSL(2,3^n)$ が成り立つ. そこで逆に, 可換なシロー2群をもつ単純群Gがあって, 位数2の元tが

$$C_G(t)=\langle t\rangle\times PSL(2,q) \qquad (q=p^n)$$

という条件をみたしている時, GはG_2型の Ree 群と同形であるかという問題がおこる. この時 $q>5$ ならば, qは3の奇数ベキでGは Ree 群とよく似た群であることが証明された.（実際にG_2型の Ree 群と同形になることはずっとあとになってから証明された(『群論』下, 英語版 p. 517 参照).）

1964年の秋 Janko が $q=5$ の場合は真に例外であって, 位数175, 560の散在単純群が存在し上述の条件をみたしていることを示し皆をあっと驚かせた. この群は Mathieu 群以来最初の散在単純群で Janko 群と呼ばれている. その後 Janko は更に三つの散在単純群が可能であることを発表したので, それらも Janko 群と呼び位数の増加順に J_1, J_2, J_3, J_4 と表わしている.

Janko [1*] はJ_1を $GL(7,11)$ の部分群として書き上げたが Livingstone [4] は266個の点からなる或るグラフを構成し, J_1をその自己同形のつくる群として表現した. J_1はこのグラフの頂点の集合に可移に作用している. そして1点の安定化群は $PSL(2,11)$ である. すなわちJ_1は $PSL(2,11)$ の原始的可移拡大となっている.

J_1の構成後間もなく Janko はさらに二つの散在単純群が可能であることを発表した. この場合, 位数2の元tの中心化群$C_G(t)$は位数2^5の esp 群, すなわち extra-special 群（『群論』下 p. 463）を5次の交代群A_5で拡大した群である. この形の中心化群をもつ単純群は交代群や Lie 型の単純群の中には存在しない. 中心化群に関する仮定の下で Janko は二つの場合が可能であること, すなわち位数2の元のつくる共役類の数が二つで $|G|=2^7 3^3 5^2 7=604,800$ となるかまたは位数2の元は一つの共役類をつくり $|G|=2^7 3^5 5\cdot 17\cdot 19=50,232,960$ となり, おのおのの場合にGの群指標の表が一意的に定まることを示した

[2*].

Janko がこの単純群が存在するであろうと発表して間もなく，M. Hall が J_2 を次数 100 の可移群として構成した．この時 J_2 は原始的で，1点の安定化群はユニタリ群 $PSU(3,3)$ に同形である．Janko によって求められた群指標の表から，J_2 は次数 100 の置換表現をもつ可能性があること，次数 100 の置換表現があるとすれば $PSU(3,3)$ が1点の安定化群になり得る群であることが見出されたのが構成のもとになっている．M. Hall は $PSU(3,3)$ から出発して，その次数 100 の可換拡大を計算機の助けをかりて構成し，それが J_2 を定義する条件をみたす唯一つの散在単純群であることを示した．位数の大きい方の Janko 群 J_3 の場合には，J_3 に含まれる部分群の位数が $|J_3|$ にくらべて小さいので，その構成は困難であった．しかし G. Higman-McKay[1*] は計算機を用いて Todd-Coxeter による剰余類数え上げ法を実行して J_3 が一意的に定まる散在単純群であることを確定した．J_2, J_3 の構成が計算機による単純群構成の始まりである．その後すぐに J_2 は 100 個の点からなる或るグラフの自己同形のつくる群として計算機なしで構成された (鈴木，Tits)．最近 J_3 も計算機の助けをかりないで構成できるようになった (Mirman-Weiss)．

Janko の群はすべて，位数2の元の中心化群の構造を与えて単純群を求めるという問題から発見されたものである．この外にも Held 群 He, Lyons 群 Ly, O'Nan 群 ON などが位数2の元の中心化群を与えることにより定義される．まず Janko 群 J_2, J_3 からしばらくたって Held 群が現われた．$PSL(5,2)$ と M_{24} においてシロー2群の中心に含まれている位数2の元をとれば，その中心化群は同形である．この中心化群を H とおこう．単純群 G においてシロー2群の中心に含まれている位数2の元の中心化群が H と同形である時，単純群 G は $PSL(5,2)$ または M_{24} と同形であるかという問題を調べているうち Held は第3の場合が可能であることを証明した [1*]．この第3の場合にあてはまる群が Held 群である．この群 He はまた G. Higman-McKay により計算機を用いて構成された．

Held 群に先だっていくつかの散在単純群がグラフの自己同形のつくる群として構成された．前に述べたように M. Hall は Janko 群 J_2 を次数 100 の置換群として計算機を用いて構成した．この結果について M. Hall が Oxford

で講演した時，丁度その場にいた D. G. Higman と Sims とが，J_2 がいわゆる階数 3 の置換群 (『群論』下 p. 879) であることに注目し，類似の方法を用いて M_{22} の次数 100 の可移拡大を構成した．すなわち，M_{22} の置換表現を三つとり (次数 1, 22, 77) それから頂点の数が 100 のグラフを作り，そのグラフの自己同形群が頂点の集合の上に可移に作用することを証明したのである．彼らは Hall の講演を聞いたあとすぐ構成にとりかかり，翌朝には新単純群ができ上っていたと伝え聞いている．この群が Higman-Sims 群 HS で，永尾 [4] に解説されている．(原論文 Higman-Sims[1*]. J_1 の構成は M. Hall-Wales[1*].)

Higman-Sims 群の構成に関する予稿を入手してから 2, 3 週間のうちに鈴木 [6*] は同様な方法を用いて階数 3 の可移拡大の系列

$$PSL(2,7)\subset PSU(3,3)\subset J_2\subset G_2(4)\subset S$$

を構成し散在鈴木群 S を発見した．ここで $G_2(4)$ は 4 元体上で定義される G_2 型 Chevalley 群である．各段階で群が階数 3 の原始置換群として作用するグラフを構成するのである．グラフの自己同形群は Aut S などと一致する．

上の系列は実は $A_6\subset PSL(3,4)\subset PSU(4,3)$ という階数 3 の可移拡大の系列の類似として構成されたものである．その構成とほとんど同時に $PSU(4,3)$ をさらに可移拡大して散在単純群が得られることを McLaughlin[1*] が証明した．この散在単純群を M^c と表わす．M^c も階数 3 の原始的置換群である．

このあとしばらくして Rudvalis[1*] が Tits 群の可移拡大となる階数 3 の原始的置換群の存在する可能性があることを発表した．その様な群が存在するとすれば位数 2 の中心をもつ中心拡大が存在し，その中心拡大は 28 次元の表現をもつことが証明された．このことから Conway-Wales[1*] は 28 次元空間のベクトルを用いて頂点数 4060 のグラフを構成し，その自己同形のつくる群として Rudvalis 群 Ru の中心拡大を構成した．この途中で計算機の助けが必要であったが，最近計算機を用いずに構成できるようになった (Weiss).

Janko 群 J_2 から始まって単純群の可移拡大としていくつかの散在単純群が構成されている間に Conway と Fischer によって別の方向から散在単純群が発見された．Conway 群は Leech 格子の自己同形の群として定義される．ずっと前から Euclid 空間に同じ大きさの球をできるだけ多くつめ込むにはどうすればよいかという問題がある．Leech は 24 次元の空間において一つの球に

非常に多くの球がふれ合っている特別なつめ方を定義した．この時，球の中心の集合は空間の格子群をつくっている．これが Leech 格子である．Conway はこの格子の原点を固定する自己同形全体がつくる群がいくつかの散在単純群を含んでいることを証明した．Conway がこの結果を得た当時の状況が MAA から出版された T. M. Thompson の書 (Carus 叢書 21) の中にドキュメンタリに述べられている．Leech 格子の原点を固定する自己同形全体を Conway にしたがって ·0 (dot 0) と呼ぶ．ベクトル v を $-v$ に移す変換 $-I$ は ·0 の中心を生成している．そこで ·0 の中心による商群を ·1 と表わす．Leech 格子に含まれる点のうち原点との距離が最小のものは 196, 560 個ある．自己同形群はこれらの点の上に可移に作用している．そのうちの 1 点の安定化群を ·2, 距離が 2 番目の点の安定化群を ·3 という．これらの群 ·1, ·2, ·3 はすべて散在単純群であって Conway 群と呼ばれている．群 ·0 は Leech 格子の自己同形群で 24 次元の直交群の部分群である．そのため各元が 24 次元の行列として具体的に表わされているので，それを用いて群の構造が調べられる利点をもっている．その上 ·0 は HS, M^c および上に述べた鈴木群に到る系列を区間として含んでいる．·0 の中で調べるのがこれらの群を研究するために一番有効な方法である．

Fischer の研究は次の群論の問題から始まった．群 G に含まれている位数 2 の元からなる共役類 D が次の条件

$$t, s \in D \Longrightarrow \text{積 } ts \text{ の位数は } 1, 2, \text{ または } 3$$

をみたしている時 D を **3 互換の共役類**という．たとえば対称群 Σ_n の中で普通の互換全体は 3 互換の共役類をつくる．また 2 元体上の直交群，斜交群，ユニタリ群では，それに含まれる移換の全体が 3 互換の共役類をつくっている．この他にも 3 元体上の直交群は 3 互換の共役類を含んでいる．Fischer は 3 互換の共役類 D から生成される有限群を調べ次の定理を証明した．

有限群 G が 3 互換の共役類 D により生成されていると仮定する．さらに G は可解な正規部分群 $\neq\{1\}$ を含まず，$G'=G''$（第 1 の交換子群と第 2 の交換子群が一致する）と仮定する．この時 G は上にあげた例（対称群，2 元体上の形式を不変にする古典群，3 元体上の直交群）のいずれかと一致するか，または $M(22)$, $M(23)$, $M(24)$ と表わされる三つの例外群のいずれかと同形になる．

この例外群 $M(22)$, $M(23)$, および $M(24)$ の交換子群 $M(24)'$ はすべて散在単純群になることも Fischer が証明した. これらの群を Fischer 群という. 例外群を $M(22)$ などと表わしたのは, それらが Mathieu 群 M_{22} などと関係しているからである.

上にあげた Fischer の定理の基本となるのは次の命題である. いま有限群 G が上定理の条件を満足していると仮定する. この時 G は D 上の置換群として階数 3 である(『群論』下 p. 900). すなわち G は $t\in D$ の中心化群の可移拡大で階数 3 の置換群となる. Fischer 群の置換群としての次数および 1 点の安定化群の構造を表しておこう.

$M(22)$	3510	$PSU(6,2)$ の中心拡大
$M(23)$	31671	$M(22)$ の中心拡大
$M(24)$	306, 936	$Z_2\times M(23)$
$M(24)'$	306, 936	$M(23)$

安定化群を中心拡大と表わした場合, どちらも中心の位数は 2 で中心拡大は非分裂拡大である. (中心拡大については『群論』上, 第 2 章 §9 を参照されたい.)

残りの散在単純群はすべて位数 2 の元の中心化群を与えることによって定義されている. 前に述べた McLaughlin 群 M^c では位数 2 の元は一つの共役類をつくることが証明される. その 1 元の中心化群は 8 次の交代群 A_8 の中心拡大であることが示された. そこで一般に交代群 A_n の中心拡大を中心化群とする単純群が存在するかどうかが問題となる. まず Janko が $n=9$ の場合は不可能であることを示した. そのあと Lyons[1*] が $n=10, 11$ の場合を調べ $n=10$ は不可能であるが $n=11$ の場合は可能であり, そのような単純群が存在すると仮定すれば, その位数は $|G|=2^8 3^7 5^6 7\cdot 11\cdot 31\cdot 37\cdot 67$ であること, またこの群は 5 元体上の G_2 型 Chevalley 群 $G_2(5)$ を部分群として含んでいることを証明した. しばらくして Sims が計算機を用いて $G_2(5)$ の可移拡大として上の条件をみたす単純群を構成した. これが Lyons 群である. ($n\geqq 12$ の場合, 交代群 A_n の中心拡大を中心化群とする単純群は存在しない.)

次に O'Nan 群について述べよう. Lyons 群が McLaughlin 群との或る類似から発見されたように O'Nan 群は Higman-Sims 群の或る部分群との類似

から発見された．Higman-Sims 群は $X \triangleright Y=(Z_4)^3$, $X/Y=SL(3,2)$（ここで Yは位数4の巡回群三つの直積）という形の部分群を含んでいることが証明される．HSではY上の拡大が分裂しているが分裂しない拡大も可能である．O'Nan 群はこの分裂しない場合のシロー2群をもつ単純群として一意的に定まる．ONは位数2の元からなる共役類を唯一つもち，その元の中心化群Cは

$$A \subset B \subset C, \qquad |C:B|=2, \quad B/A=PSL(3,4),$$

という正規列をもち，AはBの中心に含まれる位数4の巡回群である．この条件から単純群ONは一意的に定まる．またONは $PSL(3,7)$ をグラフ型の自己同形で拡大した群Lを部分群として含んでいる（O'Nan [1*]）．あとで Sims は計算機を用いてONをLの次数122,760の可移拡大として構成した．

以上述べたことが1970年代の始めまでの散在単純群の歴史的解説である．Janko 群に関連してJ_4にも触れたが Janko[3*] がJ_4の可能性について発表したのは1976年のことで1970年代はじめの時点では21個の散在単純群が発見されていた．残っている散在単純群はJ_4および Fischer-Griess の群，いわゆる monster に関係した群 F_1, F_2, F_3 および F_4 である．

これらの群について語るには当時の有限群論の様子にも触れねばなるまい．単純群分類問題についての研究は1950年代に始まったといえよう．特にその中頃に発表されたいくつかの古典的論文によって分類問題に取りかかるための準備ができ，いくつかの方法が提出された．そして1960年代の始めには懸案であった Burnside の予想の正しいことが証明された．さらに或る種の2重可移群がすっかり解明されるにおよんで，分類問題の解決へ確実に第一歩がふみ出されたといえよう．1960年代を通じて解決への道がさらに摸索されていたが，Janko群に始まる散在単純群の出現により解決の見通しがたたず混迷しているかに見えた．単純群論にとって1970年の始めは混沌の中に秩序を見出し始めた画期的な時期であったように思われる．この頃すぐれた論文が相ついで現われた．前に述べた3互換に関する Fischer の論文 [1*] もその一つである．3互換という概念は非常に特別な条件をもつために Fischer 群 $M(22)$, $M(23)$, $M(24)'$ などの散在単純群をもたらしたが，一方では2元体上の斜交群，直交群，ユニタリ群などを含むことから見られる様に或る一般性をもっている．Fischer の論文が予稿の形で発表されると Aschbacher [1] は直ちに3互

換の概念を拡張して2元体のみならず標数2の一般有限体上の斜交群，直交群，ユニタリ群，鈴木群も含めた形に Fischer の定理を拡張した．2以上の正整数からなる或る集合をσとする．位数2の元からなる共役類Dが

$$s, t \in D \Longrightarrow \text{積 } st \text{ の位数は } 1, 2, \text{ または } \sigma \text{ の数}$$

という条件をみたしている時Dをσ**互換の共役類**という．Aschbacher の拡張は3互換をσ互換と変えたものでσが奇数だけを含む場合である．また2元体上の$GL(n, 2)$において移換のつくる共役類は$\sigma=\{3,4\}$についてσ互換の共役類となっている．しかも

$$(*) \qquad st \text{ の位数が } 4 \text{ ならば } (st)^2 \in D$$

という条件をみたしている．Timmesfeld [1*] は$\{3,4\}$互換で（*）をみたす共役類から生成される有限群は Fischer の定理に現われる群および2元体上で定義された Lie 型の単純群に限ることを示した．この研究は$\sigma=\{$奇数, $4\}$の場合に拡張され，あとで単純群の分類定理の証明に重要な役目をはたすのである．分類問題に関して重要だった点は標数2の体上の Lie 型単純群を特長づける性質が発見されたことと，散在単純群がこれ以上現われなかったことである．

さて散在単純群F_1, F_2, F_3およびF_5のうち最初に現われたのはF_2，すなわち baby monster である．Fischer は$\{3,4\}$互換の共役類から生成される有限群を調べていたが前の条件（*）を仮定せずに進むと一つの散在単純群が得られる可能性のあることを証明した．$\{3,4\}$互換の共役類の元tについてその中心化群Cは正規列$A \triangleleft B \triangleleft C$をもち$|A|=|C:B|=2$，さらに$B/A$は2元体上の$E_6$型 Steinberg 群${}^2E_6(2)$である．また中心化群$C'$が次の構造をもつ位数2の元も含んでいる．すなわち，$E \triangleleft C', C'/E = \cdot 2$ (Conway 群) となりEは位数2^{23}の extra-special 群である．ずっと後になってこの様な性質をもつ散在単純群の存在することが Leon と Sims によって計算機を用いて証明された．これが Fischer 群F_2である．(Leon-Sims [1*])

Fischer と Griess は独立に，F_2の中心拡大が存在するとすれば，位数2の元tの中心化群が丁度F_2の中心拡大（中心の位数は2）となっている散在単純群Gが可能であることに気付いた．この元tはGのシロー2群の中心には含まれていない．シロー2群の中心に含まれる位数2の元をsとすれば

$$C_G(s) \triangleright E, \qquad C_G(s)/E = \cdot 1 \quad (\text{Conway 群})$$

となり，E は位数 2^{25} の extra-special 群となると予想された．このことを用いて Griess は Thompson の位数公式（『群論』下 p. 512）から G の位数が

$$|G| = 2^{46}3^{20}5^9 7^6 11^2 13^3 17\cdot19\cdot23\cdot29\cdot31\cdot41\cdot47\cdot59\cdot71$$

であることを示した．Fischer と Griess がこの群に関する研究を独立に始めたのは1973年の終末であったと伝えられている．そのあと Fischer からの情報により Thompson もこの群を調べ次の結果を得た．すなわち，この群が存在すると仮定すればその中に位数3の元 x と位数5の元 y があって

$$C_G(x) = \langle x \rangle \times F_3, \quad C_G(y) = \langle y \rangle \times F_5$$

と直積に分解し，F_3 と F_5 はそれぞれ散在単純群になる．そして Thompson はこれらの単純群 F_3, F_5 に含まれる位数2の元の中心化群の構造はそれぞれ

$$C \triangleright E, \qquad C/E = A_9, \qquad E \quad \text{extra-special}, \qquad |E| = 2^9$$

$$C \triangleright D \triangleright Z, \qquad |C:D| = |Z| = 2, \qquad D/Z = HS$$

であろうと予想した．ここで A_9 は次数9の交代群，HS は Higman-Sims 群である．しばらくして(1974年夏) Thompson は位数2の元の中心化群が上に与えた構造 (extra-special 群の A_9 による拡大) をもつ散在単純群が一意的に存在することを示した[6*]．これが F_3 である．Thompson は F_3 を $E_8(3)$（3元体上の E_8 型 Chevalley 群）の部分群として構成したので，その構成には計算機の助けが必要であった．同じ頃，原田 [2*] と Norton は F_5 がやはり位数2の元の中心化群の構造によって一意的に定まることを示し，その性質をもつ単純群を構成した．Fischer 群を F_2，Thompson 群を F_3，原田群を F_5 と表わすのは，それらが F_1 の中の位数 p の元の中心化群に含まれているからである．

F_1 の研究が始まって間もない頃から，複素数体上で F_1 の既約忠実表現の次数は少なくとも 196,883 であることが知られていた．実際に F_1 がその次数の既約表現をもつという仮定の下で Fischer, Livingstone, Thorne [2] の3人が F_1 の既約指標の表を完成することに成功した．この群指標の表から容易に 196,883 次元の表現空間は（非結合的）可換代数の構造をもち，F_1 はその代数の自己同形の群となっていることが証明される．この代数構造は Norton 代数と呼ばれている．1980年に Griess [3] はこの可換代数を計算機を用いないで

構成し，その自己同形の群として F_1 の存在証明を与えた．F_1 と共にその部分群として，F_2 の中心拡大，F_3, F_5 その他多くの散在単純群が計算機なしで構成できるようになった．

最後に Janko 群 J_4 について述べよう．この群は単純群分類定理の証明の一つの場合における例外的な振舞から現われたものである．『群論』下，第6章(p. 932)で述べたように，分類定理の証明の一部分として単純群 G が

$$Q=F^*(C_G(z)), \qquad Q \text{ は extra-special 2 群}$$

をみたす位数2の元 z を含んでいる場合を考察する必要がある．記号 $F^*(X)$ は群 X の一般化された Fitting 部分群である(『群論』下 p. 791)．多くの散在単純群がこの形の中心化群をもっている．しかし Q の位数が大きくなると例外が起らないことを Timmesfeld が証明し，単純群分類定理の証明が終りに近づいたことを皆に確信させた．Janko 群 J_4 はこの形の単純群として最後に現われた．すなわち J_4 における位数2の元の中心化群 C は次の構造をもつ．

$$C \rhd D \rhd Q=F^*(C), \qquad |C:D|=2, \qquad |Q|=2^{13}$$

さらに D/Q は Mathieu 群 M_{22} の中心拡大でその中心の位数は3である．

Janko 群 J_4 は1980年になって Cambridge の数学者達（Norton, Conway など）によって2元体上の112次の行列群として計算機を用いて構成された．

§2 散在単純群の位数

散在単純群の位数を素因数分解した形で表にしておこう．

M_{11}	$2^4 3^2 5\cdot 11$
M_{12}	$2^6 3^3 5\cdot 11$
M_{22}	$2^7 3^2 5\cdot 7\cdot 11$
M_{23}	$2^7 3^2 5\cdot 7\cdot 11\cdot 23$
M_{24}	$2^{10} 3^3 5\cdot 7\cdot 11\cdot 23$
J_1	$2^3 3\cdot 5\cdot 7\cdot 11\cdot 19$
J_2	$2^7 3^3 5^2 7$
J_3	$2^7 3^5 5\cdot 17\cdot 19$
J_4	$2^{21} 3^3 5\cdot 7\cdot 11^3\cdot 23\cdot 29\cdot 31\cdot 37\cdot 43$
HS	$2^9 3^2 5^3 7\cdot 11$

S	$2^{13}3^7 5^2 7\cdot 11\cdot 13$
M^c	$2^7 3^6 5^3 7\cdot 11$
Ru	$2^{14}3^3 5^3 7\cdot 13\cdot 29$
He	$2^{10}3^3 5^2 7^3 17$
Ly	$2^8 3^7 5^6 7\cdot 11\cdot 31\cdot 37\cdot 67$
ON	$2^9 3^4 5\cdot 7^3 11\cdot 19\cdot 31$
$\cdot 1$	$2^{21}3^9 5^4 7^2 11\cdot 13\cdot 23$
$\cdot 2$	$2^{18}3^6 5^3 7\cdot 11\cdot 23$
$\cdot 3$	$2^{10}3^7 5^3 7\cdot 11\cdot 23$
$M(22)$	$2^{17}3^9 5^2 7\cdot 11\cdot 13$
$M(23)$	$2^{18}3^{13}5^2 7\cdot 11\cdot 13\cdot 17\cdot 23$
$M(24)'$	$2^{21}3^{16}5^2 7^3 11\cdot 13\cdot 17\cdot 23\cdot 29$
F_2	$2^{41}3^{13}5^6 7^2 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 31\cdot 47$
F^3	$2^{15}3^{10}5^3 7^2 13\cdot 19\cdot 31$
F_5	$2^{14}3^6 5^6 7\cdot 11\cdot 19$
F_1	$2^{46}3^{20}5^9 7^6 11^2 13^3 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$

上にあげた散在単純群が交代群や Lie 型の単純群と同形にならないことを証明するには，位数が一致しないことを示せばよい．交代群の位数は次の性質をもっている．すなわち p を交代群の位数の素因子の一つとすれば，p より小さい任意の素数はその交代群の位数を割り切る．この命題を用いて，ほとんどすべての散在単純群の位数が交代群の位数と一致しないことがわかる．この命題によって判定できない場合，たとえば S の場合，各素数のベキを比較すればよい． $|S|$ は素数7の2乗では割り切れないから交代群 A_{13} とくらべればよい．明らかに $|S|\neq|A_{13}|$ となる．Lie 型の単純群の位数は第2, 3章において各場合に求められている． Lie 型の単純群 G が標数 p の有限体 F の上で定義されているとする．この時，素数 p はほとんどすべての場合 $|G|$ から定まってしまうのである．すなわち次の Artin の定理が成り立つ．ほとんどすべての場合に $|G|$ を割り切る最大の素数ベキは p のベキである．例外は $PSL(2,\ p)$ で p が Mersenne 素数の場合 $(l=2)$，$PSL(2, 2^r)$ で 2^r+1 が Fermat 素数の場合 $(l=2^r+1)$，その他 $PSL(2, 8)$ $(l=3)$，$PSU(3, 3)$ $(l=2)$，$PSU(4, 2)$ $(l=3)$

だけである．例外の場合書きそえた l は最大の素数ベキを与える素数である．Artin がこの定理を証明した当時は Steinberg 群など知られていなかったが，それらの新しい群を加えても同じ結果の成り立つことが証明される．この定理によって Lie 型の単純群では体 F の標数 p が位数 $|G|$ からほとんど定まる．そこで p のベキを見れば $|F|=q$ もほとんど定まる．位数の公式を眺めれば位数 $|G|$ が $q-1$ で割り切れていることがわかる．これらの事実から散在単純群の位数は Lie 型の単純群の位数と一致しないことが証明される．たとえば $|S|$ が Lie 型の単純群の位数と一致したと仮定しよう．$|S|$ を割り切る最大の素数ベキは 2 のベキだから標数は 2 である．また 2^{13} が $|S|$ を丁度割り切っている．Lie 型の単純群の位数公式から $q=2^{13}$ となる(13 個の元からなる根の正系は存在しない)．ところで $2^{13}-1$ は $|S|$ と互いに素だから矛盾が得られる．

§3 散在群の単純性

散在単純群は各群ごとに別々に定義されている．たとえば Mathieu 群は与えられた群の原始的可移拡大となる群として定義されている．したがって Mathieu 群が単純群であることは容易に証明できることであるが定義から自明というわけではない．Janko 群 J_1, J_2, J_3 などは中心化群 $C_G(t)$ が与えられた群と同形になるような位数 2 の元 t を含む単純群として定義されている(§1 参照)．しかし他の群，たとえば Fischer 群 F_2 は $\{3, 4\}$ 互換の共役類 D から生成された群で D の元 t について $C_G(t)$ の構造が与えられている．したがって F_2 が単純群になることは証明する必要がある．Janko 群の場合でも，それらの群が単純群であるとして定義しなくても，もっと弱い条件，たとえば元 t を含む共役類から生成される群であると定義しても，それらの群が単純であることを証明することができる．

この節では散在単純群をいくつかの種類に分けよう．すなわち，第 1 種の散在群は，与えられた群の原始的可移拡大として定義される群とする．第 2 種の散在群は，位数 2 の元 t を含み，その中心化群の構造が与えられた上，t を含む共役類により生成される群である．Janko 群 J_1 では更に交換子群と一致するという条件およびシロー 2 群が可換であるという条件をつけ加える．その他

の散在群のうちFischerによる3互換の共役類により生成される群またはその交換子群となるもの，すなわち $M(22), M(23), M(24)'$ を第3種，Conway群を第4種と定義する.

まず第1種の散在群が単純群であることを証明しよう．そのもととなるのは次の補題である.

(3.1)　次数 n の原始的可移置換群 G において1点の安定化群 G_a が単純群であると仮定する．この時 G は単純であるか，または G は位数 n の正規部分群 N を含み次の条件が成り立つ. $G=G_aN, G_a\cap N=\{1\}$，また N は G の極小正規部分群である. G が単純でなければ次数 n は或る単純群の位数のベキとなる.

証明　G が単純群でないと仮定して真の正規部分群を N とおく．II (2.13) により $N\not\subseteq G_a$ を得る．したがって G_aN は G の部分群で G_a より大きい．仮定により G は原始的だから G_a は G の極大部分群である．よって $G_aN=G$ が成り立つ．同形定理により $G_a\cap N$ は G_a の正規部分群となる. G_a は単純群と仮定したから $G_a\cap N=G_a$ または $G_a\cap N=\{1\}$ が成り立つ．ところで N が G_a を含んでいれば $N=G_aN=G$ となる．これは N が真の正規部分群であるという仮定に矛盾する．よって $G_a\cap N=\{1\}$ が成り立つ．同形定理により $n=|N|$ を得る．また G_a が極大部分群だから N は G の極小正規部分群である．よって N は同形な単純群いくつかの直積となり(『群論』上 p. 136 系3)，最後の主張が証明される．□

Mathieu 群 M_{22} に (3.1) を適用してみよう． M_{22} は3重可移だから原始的である(II (2.12))．1点の安定化群は前に述べたように $PSL(3,4)$ に同形だから単純群，しかも次数22は単純群の位数のベキではない(『群論』上 p. 299)．したがって (3.1) により M_{22} は単純である.

M_{23} の場合，次数が素数23であるから (3.1) により M_{23} は単純であるか，または位数23の正規部分群を含んでいる．位数23の正規部分群を含まないことは種々の方法で証明できる．たとえば，次数23の置換群では位数23の元は23巡回置換で表わされることを用いれば，位数23の部分群の正規化群は位数が高々 $22\cdot 23$ となることがわかる．したがって M_{23} は位数23の正規部分群を含まない．よって M_{23} は単純である.

Mathieu 群 M_{24} が単純であることは M_{22} の場合と同様に証明される．

小さい Mathieu 群 M_{11} の場合は 1 点の安定化群が単純ではないので (3.1) を用いることはできない．しかし (3.1) と同様に次の命題が証明される．

(3.2) 次数 n の原始的可移置換群の正規部分群 $\neq\{1\}$ の位数は $m\cdot n$ と表わすことができる．ここで m は 1 点の安定化群の正規部分群の位数である．

証明 原始的置換群 G の正規部分群 $\neq\{1\}$ を N, 1 点の安定化群を G_a とおけば $G_aN=G$ が成り立つ((3.1)の証明参照)．$G_a\cap N$ は G_a の正規部分群で $|N:G_a\cap N|=|G_aN:N|$ を得る(同形定理)．よって

$$|N|=|N:G_a\cap N|\,|G_a\cap N|=n|G_a\cap N|. \quad \square$$

Mathieu 群 M_{11} に (3.2) を適用しよう．(1 点の安定化群の真の正規部分群は位数 360 の群だから) M_{11} の真の正規部分群が存在するとすればその位数は 11 かまたは $2^3 3^2 5\cdot 11$ となる．M_{23} の場合と同様に位数 11 の正規部分群は存在しないことが証明される．位数 $2^3 3^2 5\cdot 11$ の正規部分群 H が存在すると仮定し，H のシロー 11 群を P とおく．指数 $|N_H(P):P|$ を k とおけば k は 10 の約数である．またシローの定理により $|H:N_H(P)|\equiv 1 \pmod{11}$ が成り立つ．したがって $|H:P|=360\equiv k \pmod{11}$ となるから $k\equiv 8 \pmod{11}$．これは k が 10 の約数であることに矛盾する．したがって M_{11} は単純である．

M_{11} は次数 12 の 3 重可移群として表現されることが知られている．この時 1 点の安定化群は $PSL(2,11)$ となる．この表現を用いれば (3.1) より直ちに M_{11} が単純群となることを証明できる．

Mathieu 群 M_{12} も単純である．1 点の安定化群は M_{11} だから (3.1) が使える．

Janko 群 J_2 にはじまる階数 3 の原始的可移群はすべて (3.1) を用いて，それらの群が単純群であることを証明できる．各群について次数 n と 1 点の安定化群を表にしておこう．

J_2	$2^2 5^2$	$PSU(3,3)$
HS	$2^2 5^2$	M_{22}
S	$2\cdot 3^4 11$	$G_2(4)$
M^c	$5^2 11$	$PSU(4,3)$
Ru	$2^2 5\cdot 7\cdot 29$	Tits 群

ここで $n>100$ の場合には，$p=11$ または $p=29$ についてシローの定理を用いて，位数 n の単純群が存在しないことを証明することができる．よって (3.1) により上の各群は単純である．

第2種の散在群のうち Janko 群 J_1 は特別に扱う必要がある．$G=J_1$ では位数2の元 t の中心化群 $C_G(t)$ は $\langle t\rangle\times A_5$ という形で，シロー2群は可換である．したがって $C_G(t)$ は G のシロー2群を含んでいる．このことと仮定 $G'=G$ から，位数2の元全体が一つの共役類をつくることが証明される (『群論』下 p. 514 (1.8), p. 527 (2.9))．よって G の正規部分群 N の位数が偶数ならば，$G=N$ を得る．何故ならば $|N|$ が偶数だから N は位数2の元を少なくとも一つ含み，したがって位数2の元をすべて含む．G は t を含む共役類で生成されるから $N=G$ となる．さて Janko 群 J_1 が単純でないと仮定し，極小正規部分群を M とおく．$M\neq G$ だから $|M|$ は奇数である．また $M\cap C_G(t)$ は $C_G(t)$ の正規部分群である．$C_G(t)=\langle t\rangle\times A_5$ だから $C_G(t)$ の真の正規部分群はすべて偶数位数をもつ．したがって $M\cap C_G(t)=\{1\}$ を得る．よって $|M|$ は $7\cdot11\cdot19$ の約数である．もし7が $|M|$ の約数ならば，シローの定理を用いて M のシロー7群が正規部分群となる．M は G の極小正規部分群と仮定したから，この場合は $|M|=7$．$|M|$ が7で割れない場合には同様に $|M|=11$ または19となる．いずれの場合も M は巡回群である．よって $G/C_G(M)$ は可換群となる (『群論』上 pp. 46—47 (6.9) および (6.11))．G が交換子群と一致すると仮定したので $C_G(M)$ は G と一致する．しかしこれは $C_G(t)\cap M=\{1\}$ に矛盾する．したがって Janko 群 J_1 は単純群である．Livingstone の表現によれば J_1 は次数 $266=2\cdot7\cdot19$ の原始的可移置換群で，この時，1点の安定化群は $PSL(2,11)$ である．よって (3.1) を用いて J_1 が単純であることを証明することもできる．

J_1 以外の第2種散在群が単純であることを証明するために必要な補題を二つ証明しよう．

(3.3) 有限群 G の正規部分群 N の位数が偶数と仮定する．位数2の任意の元 t について $C_G(t)\cap N\neq\{1\}$ が成り立つ．

証明 $H=C_G(t)$ とおき，H のシロー2群を Q とする．シローの定理により Q は G のシロー2群 R に含まれている．$N\lhd G$ だから $N\cap R$ は N のシロ

ー2群となる(『群論』上 p. 95, 定理2.6). 仮定により N の位数は偶数だから $N\cap R\neq\{1\}$ となる. さて同形定理により $N\cap R\lhd R$, したがって p 群の基本定理 (『群論』上 p. 83, 定理1.4) により $N\cap Z(R)\neq\{1\}$ を得る. ところで t は R の元だから $\{1\}\neq N\cap Z(R)\subset N\cap C_G(t)$ となり(3.3) が成り立つ. □

(3.4) 位数が4で割れる有限群を G とし, G に含まれている位数2の元 t について次の条件が成り立つと仮定する.

(1) $C_G(t)$ の $\{1\}$ 以外の正規部分群は t を含む.

(2) G は t の共役元全体の集合から生成される.

この時 G は単純群である.

証明 中心化群 $C_G(t)$ を H とおく. さて G が単純でないと仮定して G の真の正規部分群を N とする. まず N の位数が偶数と仮定すれば (3.3) により

$$H\cap N\neq\{1\}$$

を得る. ところで $H\cap N\lhd H$ だから条件(1)により $H\cap N$ は t を含んでいる. $N\lhd G$ より t の共役元はすべて N に含まれる. したがって条件(2)により N は G と一致する. これは N が真の部分群であるという仮定に矛盾するから N の位数は奇数である.

$H\cap N$ の位数も奇数だから(1)により $H\cap N=\{1\}$ を得る. よって N の各元 x について $txt^{-1}=x^{-1}$ が成り立つ(『群論』下 p. 517(1.9)). いま $M=C_G(N)$ とおけば M は G の正規部分群であるが G とは一致しない ($t\notin M$). したがって M の位数は奇数である.

さて $G_0=\langle M,t\rangle$ とおき, G_0 が G の正規部分群であることを証明しよう. いま $g\in G$ とすれば $gMg^{-1}=M$ が成り立つから $gtg^{-1}\in G_0$ を示せばよい. N の任意の元 x について $g^{-1}xg\in N$ だから

$$(gtg^{-1})x(gtg^{-1})^{-1}=g(g^{-1}x^{-1}g)g^{-1}=x^{-1}$$

が成り立つ. すなわち, $gtg^{-1}t^{-1}\in C_G(N)=M$, したがって $gtg^{-1}\in G_0$ を得る. このように G_0 は G の偶数位数の正規部分群である. したがって前に証明したように $G_0=G$ となる. ところで G_0 の定義から明らかに $|G_0|$ は4で割り切れないことがわかる. これは G の位数が4で割れるという仮定に矛盾する. よって G は単純群である. □

次に第2種散在群とその群を定義する中心化群の構造をのべよう.

中心化群 C を表わすために次の記号を用いる．まず記号 $2^{2n+1}X$ は正規列

$$E \lhd C, \quad C/E = X, \quad E = F^*(C)$$

をもち，E が位数 2^{2n+1} の extra-special 群となる群 C を表わす．ここで記号 $F^*(C)$ は C の一般化された Fitting 部分群（『群論』下 p. 791）である．

また Y が単純群の場合 mY は群 Y の中心拡大 D で既約かつ

$$|Z(D)| = m, \quad [D, D] \supset Z(D), \quad D/Z(D) = Y$$

をみたす群を表わす．また任意の群 Z について $Z2$ は指数 2 の部分群 Z を含み，Z の外の元は Z に位数 2 の外部自己同形を引きおこす群を表わすものと規約する．さらに $mY2 = (mY)2$ とおく．

この記号を用いて第 2 種の散在群とその群を定義する中心化群の構造を表にしておこう．（以下 J_1 は省略する．）

J_2, J_3	$2^{4+1}A^5$
J_4	$2^{12+1}(3M_{22}2)$
He	$2^{6+1}PSL(3, 2)$
Ly	$2A_{11}$
ON	$4PSL(3, 4)2$
F_2	$2(^2E_6(2))2$
F_3	$2^{8+1}A_9$
F_5	$2(HS)2$
F_1	$2F_2$

これらの散在群が単純群であることを証明するためには，上の表にあげた中心化群 C が (3.4) の条件 (1) をみたしていることを示せばよい．

まず C が $2^{2n+1}Y$ という形をしている場合を考えよう．この場合 $E = F^*(C)$ は extra-special 群である．よって E の中心 $Z(E)$ の位数は 2 で，

$$\langle t \rangle = Z(E) \qquad (C = C_G(t))$$

が成り立つ(『群論』下 p. 463)．さて D を C の正規部分群とし $D \cap E \neq \{1\}$ と仮定する．$D \cap E$ は E の正規部分群であるから p 群の基本定理により

$$D \cap E \cap Z(E) \neq \{1\}$$

を得る．ところで $Z(E) = \langle t \rangle$ だから $t \in D \cap E$，すなわちこの場合 $t \in D$ が成り立つ．次に $D \cap E = \{1\}$ と仮定しよう．$[D, E] \subset D \cap E = \{1\}$ だから D は

$C_C(E)$ に含まれる．ところで一般に $F^*(C)$ の中心化群は $F^*(C)$ に含まれる（『群論』下 p. 791 定理 6. 11）．よって $D \subset E$ となり $D = D \cap E = \{1\}$ を得る．すなわち，中心化群が $2^{2n+1}Y$ 型の場合に条件（1）が成り立つ．

C が $2X$ という中心拡大の場合には X は単純群で，この中心拡大は既約となっている．すなわち $C = Z(C)H$ をみたす部分群 H は C 以外に存在しない．そこで $D \lhd C, D \neq \{1\}, D \not\ni t$ と仮定すれば $DZ(C) \neq Z(C)$ だから $DZ(C) = C$ を得る．したがって $D = C$ となり $D \not\ni t$ と仮定したことに矛盾する．この場合も条件（1）が成り立つ．

C が $mX2$ という形の場合，$X2$ は群 X の位数 2 の自己同形による拡張であって，$X \times Z_2$ と直積に分解していない．このことから前の場合と同様に (1) の成り立つことが証明される．

第 2 種散在群が単純群であることは（3. 4）から直ちに証明される．

注意 Fischer-Griess 群 F_1 は位数 2 の他の元の中心化群によって定義することもできる．この場合，中心化群は $2^{24+1}(\cdot 1)$ と表わされる．□

Fischer 群 $M(22), M(23), M(24)$ は 3 互換全体の集合の上の置換群として階数 3 の原始置換群である．各群について次数と 1 点の安定化群の構造を再度表にしておこう．

$M(22)$	$2 \cdot 3^3 5 \cdot 13$	$2\,PSU(6, 2)$
$M(23)$	$3^4 17 \cdot 23$	$2\,M(22)$
$M(24)$	$2^3 3^3 7^2 29$	$Z_2 \times M(23)$
$M(24)'$	$2^3 3^3 7^2 29$	$M(23)$

これらの群は原始的可移拡大だから (3. 2) を用いて単純性を証明することもできる．$M(22)$ の場合，次数の 2 倍の位数をもつ単純群が存在しないことを証明する必要がある．この場合はシローの定理を $p=13$ と $p=5$ に適用して片ずけることができる．Fischer 群では 1 点の安定化群は 3 互換 t の中心化群と一致するので，(3. 4) を用いることもできる．$M(22), M(23)$ では 1 点の安定化群は既約な中心拡大だから前述の様に (3. 4) の条件 (1) が成り立ち，(3. 4) から直ちに $M(22), M(23)$ が単純であることが証明される．

$M(24)'$ は $M(23)$ の原始的可移拡大だから (3. 1) が適用される．しかしこの場合は次数が大きいのでシローの定理を今までの様に用いるだけでは $M(24)'$

が単純であることを証明できない．（群論の定理を自由に使えば位数 $2^3 3^3 7^2 29$ の単純群は存在しないことが証明できる．）

そこで（3.3）を用い，$M(24)$ の正規部分群 N を考える．$M(24)$ は原始的だから（3.1）の証明と同様にして N の位数は偶数であることがわかる．1点の安定化群を H とおけば H は3互換 t の中心化群で $H=\langle t\rangle\times M(23)$ となる．よって（3.3）により $H\cap N\neq\{1\}$．もし $H\cap N$ が t を含めば，N はすべての3互換を含む．よって $N=M(24)$ となる．そこで $H\cap N$ が t を含まないと仮定すれば H の構造から $H\cap N=M(23)$ となる．よって（3.2）により N は $M(24)$ の指数2の正規部分群である．すなわち $M(24)'$ は $M(24)$ の唯一つの真の正規部分群である．これから $M(24)'$ が単純であることが証明される．（『群論』上 p. 287 の交代群の単純性の証明を参照されたい．）

以上で Conway 群以外の散在群が単純群であることの略証を述べた．次の節で Conway 群をはっきり定義して，それらの群が単純であることを証明しよう．

§4 Conway 群

1. Mathieu 群 M_{24} Mathieu 群の性質は永尾［4］，大山［5］に詳しく述べられている．ここでは Conway 群を調べるに当って便利な形に M_{24} を定義して，この定義が通常のものと一致することを解説しよう（Conway［2*］による）．

まず23元体 F 上の線形群 $L=PSL(2,23)$ を考える．第2章§2で述べたように L は F 上の1次元射影空間の点集合に作用している．そこで F 上の2次元線形空間 V をとり，その点を縦ベクトルで表わす．射影空間の点は V に含まれる1次元部分空間であるから，それを代表するベクトルで表わし ${}^t(1,0)$ で代表される点を ∞（無限遠点），${}^t(x,1)$ が代表する点を x と表わすことにすれば（F と $\boldsymbol{Z}/23\boldsymbol{Z}$ を同一視して）

$$\Omega=\{\infty,0,1,\cdots,22\}$$

が F 上の射影直線となる．このように $L=PSL(2,23)$ を Ω 上の置換群と考えた時 L の生成元がどのような置換を引きおこしているか調べておこう．いま L の元 α,β,γ をそれぞれ次の行列に対応する元とする．

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \quad \begin{pmatrix}5 & 0\\0 & 14\end{pmatrix}, \quad \begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}.$$

計算を実行してみれば $\alpha(x)=x+1, \beta(x)=2x, \gamma(x)=-x^{-1}$ であることがわかる．ここで $\infty+1=\infty=2\infty, -0^{-1}=\infty, \infty^{-1}=0$．さて

$$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}^{-1}\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}^{-1}=\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}$$

だから $\{\alpha, \beta, \gamma\}$ が L を生成している(定理 II 2.7)．この生成集合の間に次の関係が成り立つ．

$$\alpha^{23}=1, \quad \beta^{11}=1, \quad \beta\alpha\beta^{-1}=\alpha^2, \quad \gamma\beta\gamma^{-1}=\beta^{-1}.$$

集合 Ω を二つの部分集合 Q と N とに分ける．Q は平方元の集合

$$Q=\{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

で　$N=\Omega-Q$ である．β は Q, N を不変にする．また

$$Q'=Q-\{0\}, \qquad N'=N-\{\infty\}$$

とおけば $\langle\beta\rangle$ は Q' 上に可移に作用している．N' の上にも可移である．

さて Ω 上の置換 δ を $x\in Q$ の時 $\delta(x)=x^3/9$, $x\in N$ の時 $9x^3$ と定義する．δ を巡回置換の積に分解しておこう．

$$\begin{aligned}\delta=&(\infty)(3)(1, 18, 4, 2, 6)(8, 16, 13, 9, 12)\\&(0)(15)(22, 14, 17, 11, 19)(20, 10, 7, 5, 21).\end{aligned}$$

上の記号において上段の元 a の下は $-a^{-1}$ である．よって δ は γ と可換で

$$\delta\beta\delta^{-1}=\beta^3$$

が成り立つ．積 $\gamma\delta$ の位数は 10 で，γ も δ も $\gamma\delta$ のベキとなる．さて

$$M=\langle\alpha, \beta, \gamma, \delta\rangle=\langle\alpha, \beta, \gamma\delta\rangle$$

とおき，M が M_{24} と同形であることを証明しよう．

(4.1)　M は Ω 上 5 重可移に作用する．

証明　$L=PSL(2, 23)$ は Ω 上に 2 重可移に作用する(定理 II 2.8)．したがって M も 2 重可移である．

さて M は $(1^3, 7^3)$ 型の置換を含んでいる．たとえば $\alpha^2\delta$．よって 2 点の安定化群は $(1^2, 11^2)$ 型の置換および $(1^3, 7^3)$ 型の置換を含むから，残りの 22 点の上に可移に作用する．すなわち M は 3 重可移である．

3 点の安定化群は $(1^3, 7^3)$ 型の置換および $(1^4, 5^4)$ 型の置換を含んでいるか

ら残りの21点の上に可移に作用する．すなわちMは4重可移である．

計算により$\alpha^2\gamma\delta$は(12^2)型であることがわかる．よって$(\alpha^2\gamma\delta)^3$は(4^6)型である．4点が与えられた時，この4点を全体として不変にする部分群Hは$(1^4 5^4)$型および(4^6)型の置換を含んでいる．よってHは残りの20点の上に可移，すなわち，Mは5点からなる部分集合全体の上に可移に作用する．

そこで5点がつくる集合Δを一つ定め，Δを全体として不変にする部分群を考えよう．δの共役元を適当にとればその元はΔ上に5巡回置換として作用する．Δ上に互換として作用する元があることを示すため，いま一度，置換の積を計算する．$\alpha\delta$は$(1^2 2^2 3^2 6^2)$型の置換だから$(\alpha\delta)^3$は$(1^8 2^8)$型である．よってその共役元を適当にとればΔ上に互換として作用する元が得られる．5巡回置換と互換は対称群Σ_5を生成する．すなわちMはΔ上にΣ_5を引きおこす部分群を含んでいる．Mは5点からなる部分集合全体の上に可移だからMは5重可移である．□

つぎにMが交代群A_{24}と一致しないことを示そう．Ωの部分集合の全体を$\mathcal{P}(\Omega)$と表わす．$\mathcal{P}(\Omega)$の中に8元からなる部分集合の族を定義してそれが$5(24, 8, 1)$デザインとなることおよびMがそのデザインの自己同形群となることを証明する．

まず$\mathcal{P}(\Omega)$は2元体上の線形空間と考えられる．すなわち二つの部分集合SとTとの和はSとTの対称差，$S+T=(S\cup T)-(S\cap T)$，と定義する．$\mathcal{P}(\Omega)$の元を次の様に24次元のベクトル

(4.2)　$$S=(a_\infty, a_0, a_1, \cdots, a_{22})$$

の形で表わす．ここで$i\in S$の時$a_i=1$，$i\notin S$の時$a_i=0$とする．この表示を2元体上のベクトルと考えれば$S+T$は丁度ベクトルの加法と一致する．すなわち$\mathcal{P}(\Omega)$は2元体上の24次元の線形空間Vとなる．そこでΩの部分集合をVの元と考えることにする．

定義 4.3　$N_\infty=\Omega,\quad N_0=N,\quad N_i=\{n-i\mid n\in N\}$

とおく．ここでNは前に定義したように非平方元の全体である．$\{N_i\}$が生成するVの部分空間を$\mathcal{C}$と定義する．$\mathcal{C}=\langle N_\infty, N_0, \cdots, N_{22}\rangle$．任意の部分集合$S$に対し$\varphi(S)=\sum_{i\in S}N_i$とおく．□

Vの中で$2N_i=0$が成り立つから$\varphi(S+T)=\varphi(S)+\varphi(T)$を得る．すなわ

ち φ は V から $\mathscr{C}$ の中への準同形である．

まず $\varphi(N_\infty)=\varphi(N_i)=0$ が成り立つことを示そう．$\varphi(\Omega)=\sum N_i$ の右辺に Ω の各元が現われる回数を数える．集合として $\{\Omega, n-i\}$ であるからすべての平方元は同一回数現われる．非平方元についても同様である．よって上式の右辺は各元の現われる回数を係数にして

$$24\{\infty\}+12\{0\}+aQ'+bN'$$

と表わすことができる．元数を数えて $24+12\cdot 23=24+12+(a+b)11$，すなわち $a+b=24$ を得る．明らかに 1 は 12 回現われるから $a=b=12$ となる．よって $\varphi(N_\infty)=0$ が成り立つ．$\varphi(N_0)$ の場合は $\{\Omega, n-n'\}$ ここで n, n' は共に非平方元である．前と同様に $12\{\infty\}+12\{0\}+cQ'+dN'$ となり $c+d=12$ が成り立つ．さて

$$N_0=\{\infty, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

だから 1 は非平方元の差として 5 通りに表わされる（$1=22-21$ など）．Ω の中にも一度現われるから 1 は 6 回現われることになり $c=d=6$．すなわちこの場合も $\varphi(N_0)=0$ が成り立つ．$N_i=\alpha^{-i}(N_0)$ だから $\varphi(N_i)=0$ を得る．

(4.4)　(i)　$\dim\mathscr{C}=12$．$S\in\mathscr{C}\Leftrightarrow\varphi(S)=0$．

(ii)　12 個の元 N_∞ および N_i $(i\in Q')$ が $\mathscr{C}$ の基となる．

証明　定義により $\mathscr{C}=\operatorname{Im}\varphi$ が成り立つ．そこで $\dim\mathscr{C}=k$ とおけば

$$\dim\ker\varphi=24-k.$$

ところで上に証明したように $\mathscr{C}\subset\ker\varphi$ が成り立つから $k\leqq 24-k$，すなわち $k\leqq 12$ となる．そこで N_∞, N_i $(i\in Q')$ が一次独立であることが証明できたとすれば $\mathscr{C}$ の次元は少なくとも 12 となる．よって $k=12$，さらに $\mathscr{C}=\ker\varphi$ および (ii) が成り立つ．

さて N_∞, N_i $(i\in Q')$ が一次独立であることを証明するには，各 N_i をベクトル (4.2) の形に表わした時，それらのつくる行列の階数が 12 であることを示せばよい．最後に $i-1$ 個の 0 が並ぶベクトルが $i=0$ から $i=11$ まで部分空間 $\langle N_\infty, N_i\ (i\in Q')\rangle$ に含まれていることを確かめればよい．そのようなベクトル（の一つ）B_i を $B_0=N_\infty, B_1=N_1, B_2=N_2$ からはじめて N の添数が大きくなる順に計算して行けば $B_3=N_3, B_4=N_4, B_5=N_\infty+N_1+N_6$ など B_{11} まで存在する．よって $\{N_\infty, N_i\ (i\in Q')\}$ は一次独立である．□

(4.5)　群 M は部分空間 $\mathscr{C}$ を不変にする.

証明　M の生成元として α, β および $\gamma\delta$ をとることができる. さて

$$\alpha(N_\infty)=N_\infty,\quad \alpha(N_i)=N_{i-1},\quad \beta(N_\infty)=N_\infty,\quad \beta(N_i)=N_{2i}$$

が成り立つから α も β も $\mathscr{C}$ を不変にする. 元 $\gamma\delta$ は $\langle\beta\rangle$ を正規化する. 実際, $\gamma\delta\beta(\gamma\delta)^{-1}=\beta^{-3}=\beta^8$ となる. 明らかに $\gamma\delta(N_\infty)=N_\infty$ が成り立つ. 任意に $i\in Q'$ をとれば $\langle\beta\rangle$ が Q' 上可移だから $N_i=\beta^k(N_1)$ となる. よって

$$(\gamma\delta)(N_i)=\beta^{8k}(\gamma\delta)N_1$$

となる. そこで $(\gamma\delta)N_1\in\mathscr{C}$ が証明できれば $\gamma\delta$ も $\mathscr{C}$ を不変にすることがわかり (4.5) が証明される. $(\gamma\delta)N_1$ を (4.2) の形のベクトルで表わした時それが $\{N_i\}$ の一次結合に書けることを示せばよい. 実際

$$(\gamma\delta)N_1=\varphi(S),\quad ここで\ S=\{\infty,6,8,13,16,18\}\qquad \square$$

注意　(4.4)の証明において $B_i=\varphi(S_i)$ $(i=0,\cdots,11)$ をみたす部分集合 S_i を一つずつ定めておけば (4.5) の証明における S を容易に求めることができる. さらに $S_{10}=\{\infty,4,8,9\}$ に対し

$$B_{10}=\{0,1,2,3,4,7,10,12\}$$

は $\{0,1,2,3,4\}$ を含む8元集合であることもわかる. また

$$B_{11}=\{\infty,0,2,4,5,6,10,11\}\in\mathscr{C}.\quad \square$$

定義 4.6　$\mathscr{C}\subset\mathscr{P}(\Omega)$ であるから $\mathscr{C}$ の部分集合

$$\mathscr{C}_n=\{S\in\mathscr{C}\mid |S|=n\}$$

が定義される. 特に $\mathscr{C}_8=\mathscr{D}$ とおく. $\square$

以下 $\mathscr{D}$ が 5(24, 8, 1) デザインであることを証明しよう. そのため次の補題を証明する.

(4.7)　任意の $S, T\in\mathscr{C}$ について $S\cap T$ は偶数個の点を含む.

証明　$\mathscr{C}$ の元を (4.2) の形に表現する. この時 $S\cap T$ の元数が奇数であるか偶数であるかは, 2元体上の内積 (S, T) が1か0かによって定まる. さて内積は α, β により不変. したがって $i\neq\infty$ ならば

$$(N_i, N_j)=(N_0, N_{j-i}),\quad (N_0, N_i)=(N_0, N_{2i})$$

をみたす. 明らかに $(N_\infty, N_i)=(N_0, N_1)=(N_0, N_{-1})=0$ が成り立つからすべての i, j について $(N_i, N_j)=0$ となる. このことから任意の $S, T\in\mathscr{C}$ について $(S, T)=0$ となる. すなわち $|S\cap T|$ は偶数である　$\square$

(4.8)　$S\in\mathscr{C}$ に含まれる点数は4で割り切れる.

証明 $\mathcal{C}_0=\{S\in\mathcal{C}\,|\,|S|\equiv 0 \pmod 4\}$ とおく．N_i の元数は 12 の倍数だから $\mathcal{C}_0$ は $\mathcal{C}$ の一つの基を含んでいる．いま $S\in\mathcal{C}_0$, $T\in\mathcal{C}_0$ とすれば (4.7) により $|S\cap T|$ は偶数．したがって $|S+T|\equiv|S|+|T| \pmod 4$ が成り立つ．すなわち $\mathcal{C}_0$ は $\mathcal{C}$ の部分空間である．よって $\mathcal{C}_0=\mathcal{C}$ となり (4.8) が成り立つ． ▯

(4.9) $S\in\mathcal{C}\Rightarrow|S|\neq 4$. したがって $|S|=0, 8, 12, 16$ または 24.

証明 $S=\{a, b, c, d\}\in\mathcal{C}$ と仮定する．群 M は Ω 上 5 重可移だから M は $a\to a, b\to b, c\to c$ だが d を S の外に移す元 σ を含んでいる．M は $\mathcal{C}$ を不変にするから (4.5) $\sigma(S)\in\mathcal{C}$. よって $S+\sigma(S)\in\mathcal{C}$. 定義から明らかに $|S+\sigma(S)|=2$ となるから，これは (4.8) に矛盾する． ▯

定理 4.10 $\mathcal{D}$ は 5(24, 8, 1) デザインである．M は $\mathcal{D}$ の自己同形群 M_{24} と一致する．

証明 前に注意したように 5 点 $\{0, 1, 2, 3, 4\}$ を含む $\mathcal{D}$ の元が存在する．以下 $\mathcal{D}$ の元を**ブロック**と呼ぶ．M は $\mathcal{C}$ を不変にする 5 重可移群であるから，任意に Ω から 5 点をとれば，その 5 点を含むブロックが少なくとも一つ存在する．与えられた 5 点を含むブロックが S, T と二つ存在すると仮定すれば $S+T$ は $\mathcal{C}$ の元であるが $S+T\neq 0$, $|S+T|\leqq 6$ となる．これは (4.9) に矛盾する．したがって与えられた 5 点を含むブロックは唯一つ存在する．すなわち $\mathcal{D}$ は 5(24, 8, 1) デザインである（永尾 [4] p.16, 大山 [5] p.121）.

大山 [5] p.159 定理 5.5 により $\mathcal{D}$ は Witt 系 W_{24} と同形で，その自己同形群は M_{24} である（大山 [5] p.161 定理 5.6）．明らかに $M\subset M_{24}$ となる．前に計算したように $(\alpha\delta)^3$ は $(1^8, 2^8)$ 型，$(\alpha\delta)^2$ は $(1^6, 3^6)$ 型だから M において 5 点の安定化群の位数は少なくとも 6 となる．よって M の指数 $|M_{24}:M|$ は高々 8 となる．ところで M_{24} は単純群だから指数が 23 以下の真の部分群をもつことはできない．よって $M_{24}=M$ を得る． ▯

注意 $\mathcal{C}$ は Golay code の一つである．すなわち $\mathcal{C}$ の元を (4.2) のベクトルの形に書いて一つの暗号と考える．このように $\mathcal{C}$ を**符号系**と考えれば，$\mathcal{C}$ は次の性質をもっている．$\mathcal{C}$ の元 S を伝送した時，伝送中の事故などにより受信側ではもとの元と多少異なるベクトル T を受けとる．もとの元とちがっている座標の数 $|S+T|$ は符号間の Hamming の距離といわれるもので，長さのみたすべき性質をもっている．(4.9) により $\mathcal{C}$ の 2 元の間の距離は少なくとも 8 だから，伝送中に起る誤りが高々 3 個ならば，T からもとの $\mathcal{C}$ の元 S を一意的に定めることができる．すなわち，$\mathcal{C}$ は 3 個の誤りの訂正できる

符号系である． □

2. Conway 群 まず Leech 格子を定義しよう．$\mathcal{C}$ および $\mathcal{D}$ はそれぞれ定義4.3, 4.6において定義された通りとする．

定義 4.11 24次元 Euclid 空間 $\boldsymbol{R}^{24}$ に正規直交基 $\{v_i\}$ をとる．ここで添数 i は前節同様 $\Omega=\{\infty, 0, 1, \cdots, 22\}$ に属するとする．任意の $S\subset\Omega$ について $v_S=\sum_{i\in S}v_i$ とおき $2v_D$ $(D\in\mathcal{D})$ が生成する格子群を $\varDelta$ とおく．Leech 格子 $\varLambda$ は $v_\Omega-4v_\infty$ と $\varDelta$ が生成する格子群である．

$\boldsymbol{R}^{24}$ における内積を (x, y) と表わし $\varLambda_n$ を次のように定義する．

$$\varLambda_n=\{x\in\varLambda\,|\,(x, x)=16n\}. \quad □$$

格子群 $\varLambda$ とその自己同形群を調べるために必要となる $\mathcal{C}$ や $\mathcal{D}$ の性質について述べよう．

(4.12) $\mathcal{D}$ は $\mathcal{C}$ を生成する．

証明 前に注意したように $B_{10}\in\mathcal{D}$ となる．したがって $\alpha^i(B_{10})$ $(i=0, 1, \cdots, 10)$ は一次独立ですべて $\mathcal{D}$ の元である (4.5)．これに $B_{11}\in\mathcal{D}$ を加えて $\mathcal{C}$ の基が得られる((4.4) (i) 参照)．よって $\mathcal{D}$ は $\mathcal{C}$ を生成する． □

(4.13) 4点からなる集合を T とする．この時 Ω を六つの4点集合 $\{T_i\}$ に分割して $T_0=T$, 任意の i と $j\neq i$ について $T_i\cap T_j$ は空集合，さらに

$$T_i\cup T_j\in\mathcal{D}$$

をみたすようにできる．この分解は一意的に定まる．(これを T が定める**分割**，くわしく言えば **6×4 分割**という．)

証明 T に含まれない元 x を定めれば $\{T, x\}$ を含むブロックが一意的に定まる．このように T を含むブロックは丁度5個存在する．それを $\{T, T_i\}$ $(i=1, 2, \cdots, 5)$ とおけば $T_0=T, T_1, \cdots, T_5$ は上にあげた性質をもつ．すなわち

$$T_i\cup T_j=(T\cup T_i)+(T\cup T_j)\in\mathcal{D}. \quad □$$

(4.14) 元 $\sum x_iv_i$ が $\varDelta$ に属するための条件は各係数 x_i が偶数，$\sum x_i$ は16の倍数，さらに x_i が4で割り切れない添数 i のつくる集合は $\mathcal{C}$ の元となることである．

証明 上の条件をみたす $\varDelta$ の元の全体は明らかに $\varDelta$ の部分群をつくる．ところで $\varDelta$ の生成元 $2v_D$ $(D\in\mathcal{D})$ は上の3条件をみたすから，$\varDelta$ の各元は上にあげた条件をみたしている．逆を証明するために2, 3の補題を証明する．

(i)　4 点集合 T を任意にとれば $4v_T\in\Delta$. これは次のように証明される. T が定める 6×4 分割を $\{T_i\}$ とする. この時 v_T などを (T) と表わせば

$$4(T)=2(T\cup T_1)+2(T\cup T_2)-2(T_1\cup T_2)\in\Delta.$$

(ii)　任意の i,j $(i\neq j)$ について $4(v_i-v_j)\in\Delta$. (適当に 4 点集合 T と T' をとれば $4(v_i-v_j)=4(T)-4(T')$ と書ける.)

(iii)　任意の i について $16v_i\in\Delta$. (i を含まない 4 点集合 T をとれば

$$16(i)=\sum_{j\in T}4((i)-(j))+4(T)\in\Delta.)$$

さて $x=\sum x_iv_i$ が(4.14)の 3 条件をみたしていると仮定する. x_i が 4 で割り切れない添数 i のつくる集合を S とおけば S は $\mathcal{C}$ の元である. よって(4.12)により $S=\sum D_i$ $(D_i\in\mathcal{D})$ となる. そこで $y=x-\sum 2(D_i)$ とおけば y の各係数 y_i は 4 の倍数, そして $\sum y_i$ は 16 の倍数となる. ところで $y=\sum y_i(v_i-v_0)+(\sum y_i)v_0$ だから (ii) および (iii) により $y\in\Delta$, したがって $x\in\Delta$ を得る. □

Leech 格子 Λ について同様の結果が成り立つ.

(4.15)　元 $\sum x_iv_i$ が Leech 格子 Λ に属するための条件は次の三つである.

(i)　x_i はすべて偶数かまたはすべて奇数である.

(ii)　係数 x_i が法 4 の与えられた剰余類に入る添数の集合は $\mathcal{C}$ の元である.

(iii)　x_i がすべて偶数ならば和 $\sum x_i$ は 8 の倍数, x_i がすべて奇数ならば和は 8 を法として 4 に合同となる.

証明　Δ の元および $v_\Omega-4v_\infty$ は上の条件をみたす. したがって Λ の各元は条件 (i)—(iii) をみたしている. 逆に $x=\sum x_iv_i$ が上の条件をみたしていると仮定し, x_i が奇数の時 $m=1$, 偶数の時 $m=0$ とおく. さて

$$y=x+l(v_\Omega-4v_\infty)=\sum y_iv_i$$

とおけば $\sum y_i=4m+8k+20l$ と $y_i\equiv m+l \pmod 2$ とが成り立つ. そこで $m+l\equiv 2k \pmod 4$ をみたす l をとれば $\sum y_i\equiv 0 \pmod{16}$ で各 y_i は偶数となる. しかも y_i が 4 で割り切れない添数の集合は $\mathcal{C}$ の元である. よって (4.14) により $y\in\Delta$, すなわち $x\in\Lambda$ を得る. □

(4.16)　$x\in\Lambda$ ならば内積 (x,x) は 16 で割り切れる.

証明　まず x,y が Λ の生成元ならば (x,y) は 8 の倍数である((4.7)参照). したがって任意の x,y について内積 (x,y) は 8 の倍数となる. このことから (x,x) が 16 の倍数となる元 x の全体は Λ の部分群をつくることがわかる. と

ころで任意の生成元 z について $(z,z)=32$ となるから (4.16) が成り立つ. □

この命題により Λ は $\Lambda_1, \Lambda_2, \Lambda_3, \cdots$ の和集合となる. 容易に証明されるように Λ_1 は空集合である. 任意の i, j $(i \neq j)$ について $\pm 4v_i \pm 4v_j$ は (任意の符号で) Λ_2 の元である. また任意にブロック $D \in \mathscr{D}$ をとれば

$$\textstyle\sum_{i \in D} \pm 2v_i \qquad (\text{負号の数は偶数})$$

は Λ_2 の元である. 負号の数に関する制限は係数和が 8 の倍数となることによる. 奇数係数の場合, 任意の $k \in \Omega$ について

$$\textstyle\sum_{i \neq k} \pm v_i \mp 3v_k$$

において下段の符号をとる添数の集合が $\mathscr{C}$ の元である時この元も Λ_2 に含まれている. これらの元をそれぞれ (4^2) 型, (2^8) 型, $(-3, 1^{23})$ 型の元という.

(4.17) 上にあげた元以外に $\Lambda_1 \cup \Lambda_2$ の元はない.

証明 $x = \sum x_i v_i \in \Lambda_1 \cup \Lambda_2$ とすれば $\sum x_i^2 = 16$ または 32 である. いま x_i が奇数とすれば各 x_j は奇整数だから唯一つの係数が ± 3 で残りはすべて ± 1 となる. すなわち x は $(-3, 1^{23})$ 型である. つぎに x_i は偶数であるがその中に 4 で割り切れない係数があると仮定する. (4.15) (ii) と (4.9) により少なくとも 8 個の添数について係数が 0 でない. 各係数は偶数だから x は (2^8) 型である. 最後にすべての係数 x_i が 4 の倍数ならば $\sum x_i$ は 8 の倍数だからこの場合 x は (4^2) 型である. □

(4.18) (4^2) 型の元の数は $2^2(24 \cdot 23/2)$, (2^8) 型の元数は $2^7 \cdot 759$, そして $(-3, 1^{23})$ 型の元数は $24 \cdot 2^{12}$ である. Λ_2 は $196,560 = 2^4 3^3 5 \cdot 7 \cdot 13$ 個の元を含んでいる.

証明 $\mathscr{D}$ のブロックの数は 759 である (大山 [5] p. 160). したがって (2^8) 型の元の総数は $2^7 \cdot 759$ となる (2^7 だけ符号のつけ方がある). $\mathscr{C}$ の元数は 2^{12} である (4.4). $(-3, 1^{23})$ 型の元において -3 は任意の座標の係数となる. その上で符号のつけ方が 2^{12} 通りあるから $(-3, 1^{23})$ 型の元数は $24 \cdot 2^{12}$ である. (4^2) 型の元数は容易に求められる. (4.17) により $|\Lambda_2| = 196,560$ を得る. □

同様にして Λ_3, Λ_4 に含まれる元の型と, その型の元数が定められる.

(4.19) Λ_3 に含まれる元の型とその型の元数は次の通りである.

$(4, 2^8)$:	係数 ± 2 は $\mathscr{D}$ の元, -2 の数は奇数 ;	$2 \cdot 16 \cdot 759 \cdot 2^7$
(2^{12}) :	係数 ± 2 は $\mathscr{C}_{12}$ の元, -2 の数は偶数 ;	$2576 \cdot 2^{11}$

$(5, 1^{23})$:	負号は $\mathscr{C}$ の元；	$24\cdot 2^{12}$
$(-3^3, 1^{21})$:	“負号”は $\mathscr{C}$ の元；	$2^{12}(24\cdot 23\cdot 22/6)$

$|\Lambda_3| = 2^{12}3^2 5\cdot 7\cdot 13 = 16,773,120.$ □

ここで“± 2 は $\mathscr{D}$ の元”は係数が ± 2 の項の添数の集合が $\mathscr{D}$ の元であることを略したものである．$(-3^3, 1^{21})$型の場合“負号”とは係数が -1 または $+3$ になることである．(4.9) により $|\mathscr{C}_{12}| = 2^{12} - 2 - 2\cdot 759 = 2576$ となる．

(4.20) Λ_4 に含まれる元の型とその型の元数は次の通りである．

(8)		$2\cdot 24$
$(6, 2^7)$	非零係数は $\mathscr{D}$ の元，負号の数は奇数；	$759\cdot 8\cdot 2^7$
(4^4)		$2^4(24\cdot 23\cdot 22\cdot 21/4!)$
$(4^2, 2^8)$	± 2 は $\mathscr{D}$ の元，-2 の数は偶数；	$2^2(16\cdot 15/2)759\cdot 2^7$
$(4, 2^{12})$	± 2 は $\mathscr{C}_{12}$ の元，-2 の数は奇数；	$2576\cdot 2^{11}\cdot 12\cdot 2$
(2^{16})	± 2 は $\mathscr{C}_{16}$ の元，-2 の数は偶数；	$759\cdot 2^{15}$
$(5, -3^2, 1^{21})$	“負号”は $\mathscr{C}$ の元；	$(24\cdot 23\cdot 22/2)2^{12}$
$(-3^5, 1^{19})$	“負号”は $\mathscr{C}$ の元	$(24\cdot 23\cdot 22\cdot 21\cdot 20/5!)2^{12}$

$|\Lambda_4| = 2^4 3^7 5^3 7\cdot 13 = 48(8,292,375).$ □

Conway 群 $\cdot 0$ は原点を固定する回転群の部分群で Leech 格子 Λ を不変にする群として定義される．

次の定理が Conway 群の重要な性質の一つである．

定理 4.21 Conway 群 $\cdot 0$ の元を正規直交基 $\{v_i\}$ を用いて行列表示すれば成分が有理数の直交行列により表現される．行列の成分に現われる分母は 8 の約数である．

証明 任意の j について $8v_j \in \Lambda$ だから $8v_j$ の像は $\{v_i\}$ の整係数一次結合となる．よって $\cdot 0$ の元は分母が 8 の約数である有理数を成分とする行列により表現されている． □

定義 4.22 任意の部分集合 $T \subset \Omega$ に対し符号変換 ε_T を

$$\varepsilon_T(v_i) = v_i \quad (i \notin T), \qquad \varepsilon_T(v_i) = -v_i \quad (i \in T)$$

と定義し，$E = \{\varepsilon_S\}$ $(S \in \mathscr{C})$ とおく．任意の $\pi \in M$ に対し座標変換

$$v_i \longmapsto v_{\pi(i)}$$

を対応させ，それも同じ文字 π で表わす． このように M を直交群の部分群と

考え $N=EM=\{\varepsilon_S\pi \mid S\in\mathcal{C}, \pi\in M\}$ とおく．（Mは§4.1で定義した群.） □

(4.23) 次の関係が成り立つ．$\varepsilon_S\varepsilon_T=\varepsilon_{S+T}$ および

$$(\varepsilon_S\pi)(\varepsilon_T\rho)=\varepsilon_S\varepsilon_{\pi(T)}\pi\rho.$$

EおよびMは$\cdot 0$の部分群で，NはEとMとの半直積である．EはNの正規部分群で $E\cong\mathcal{C}$，よって $|N|=2^{22}3^3 5\cdot 7\cdot 11\cdot 23$ となる．

証明 $\varepsilon_S\varepsilon_T=\varepsilon_{S+T}$ および $\pi\varepsilon_T\pi^{-1}=\varepsilon_{\pi T}$ が成り立つことは明らかである．よって $S\longmapsto\varepsilon_S$ は$\mathcal{C}$からEの上への準同形写像で，この写像により$\mathcal{C}$はEと同形になる．Mは$\mathcal{C}$を不変にしているからMはEを正規化する．よってNは部分群でEとMとの半直積となる．

Nが$\cdot 0$の部分群であることを示すにはNの元がΛの生成元をΛの中に移すことを示せばよい．Mは$\mathcal{D}$の自己同形群だから $\pi\in M$ は生成元$2v_D$を$2v_{\pi(D)}$ に移す．またπが $v_\Omega-4v_\infty$ をΛの元に移すことも明らかである．符号変換ε_SはSの元に対応する座標の符号を変える．ところで $S\in\mathcal{C}$ だから任意の $D\in\mathcal{C}$ に対して $|S\cap D|$ は偶数である(4.7)．よって $\varepsilon_S(2v_D)\in\Lambda$ となる((4.18)参照)．$\varepsilon_S(v_\Omega-4v_\infty)\in\Lambda$ も明らかである．したがってNは$\cdot 0$の部分群となる．

$|E|=|\mathcal{C}|, |M|=|M_{24}|$ だからNの位数が上にあげた数になる． □

(4.24) $\cdot 0$の元λが或る i,j について $\lambda v_i=\pm v_j$ をみたしていればλはNの元である．

証明 λを表現する行列Lを考える．仮定によりi番目の列はj番目の成分が ± 1，残りの成分は0となる．Lは直交行列だから他の列のj番目の成分は0である．$k\neq i$ とし $4v_i+4v_k$ のλによる像を考える．これはLのi番目の列とk番目の列の和の4倍であるから像のj成分は ± 4 である．一方，その像はΛ_2の元であるから (4^2) 型である(4.17)．したがってk番目の列もただ1か所だけ ± 1 で他の成分は0，すなわち $\lambda=\varepsilon_S\pi$ という形をしている．ここでSはΩの部分集合，πはΩの置換である．$\lambda\in N$ を証明しよう．

さて $D\in\mathcal{D}$ とすれば $\lambda(2v_D)$ の非零成分はπDの上にのっている．よって $\lambda(2v_D)\in\Lambda$ より $\pi D\in\mathcal{D}$ を得る．すなわち，πは$\mathcal{D}$の自己同形を与える．よって定理4.10により $\pi\in M$ となる．$\lambda(v_\Omega-4v_\infty)$ において“負号”はSの上でおこる．よって (4.15) により $S\in\mathcal{C}$ を得る． □

定理 4.25 Nは $\cdot 0$ の真の部分群である.

証明 任意に4元集合 $T\subset\Omega$ をとる. この時, 次のようにして $\cdot 0$ の元 ξ_T が構成できる. Tが定める 6×4 分割を $\{T_i\}$ とおく((4.13)参照). さて

$$P=a\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix} \qquad a=1/2$$

は4次の直交行列である. $\boldsymbol{R}^{24}$ の基を $T_0, T_1, \cdots, T_5$ の分割に適合するように並べた時 Pが対角線に沿って6個並ぶ行列により表現される変換を η とおく. η によって Λ の生成元がどう変換されるかを調べよう.

いま $D\in\mathscr{D}$ をとればDの元はTによる 6×4 分割の各元に分配される. 任意の $i\neq j$ について $T_i\cup T_j$ は$\mathscr{D}$の元だからDとの共通部分は 0, 2, 4 または 8個の元を含んでいる((4.7) および5点を含むブロックの一意性). したがってDの元が分配される仕方は (4^2), (2^4), または $(3, 1^5)$ である. その各場合に $\eta(2v_D)$ を計算すれば $\eta(2v_D)$ は

(4^2) の場合 $(-2, -2, -2, -2)^2(0, 0, 0, 0)^4$

(2^4) の場合 $(0, 0, -2, -2)^4(0, 0, 0, 0)^2$

$(3, 1^5)$ の場合 $(-1, -1, -1, -3)(1, -1, -1, -1)^5$

となる. 同様に $\eta(v_\Omega-4v_\infty)=(-3, 1, 1, 1)(-1, -1, -1, -1)^5$ となる. ここで最初の二つは Λ の元であるが最後の二つは Λ の元ではない. "負号" のついた項が $\mathscr{C}$ の元の上にのっていないからである. しかし, 6×4 分割に含まれる任意の T_i 上で符号を変えれば Λ の元が得られる. これは $(3, 1^5)$ の場合以外は明らかである. $(3. 1^5)$ の場合, 最初の項の符号を変えれば負号は D の補集合の上でおこり, 第2項の符号を変えれば負号はDと $T_0\cup T_1$ の和の補集合の上でおこる. よって $\xi_T=\varepsilon_T\eta$ は $\cdot 0$ の元である. Nの元は単項行列で表現されるから, $\xi_T\notin N$ となり定理が証明される. □

定理 4.26 Conway 群 $\cdot 0$ は Λ_2 に可移に作用する. また Λ_3, Λ_4 の上にも可移に作用している. 部分群 Nの指数は奇数 $3^6 5^3 7\cdot 13$ である. したがって

$$|\cdot 0|=2^{22}3^9 5^4 7^2 11\cdot 13\cdot 23.$$

証明 任意の2点 i, j $(i\neq j)$ が与えられた時 $i\in T, j\notin T$ をみたす4点集合 Tをとり前定理の証明において構成した元 ξ_T を考える. この時 ξ_T は $\pm 4v_i$

$\pm 4v_j$ を (2^8) 型の元に移す．

次に(2^8)型の元 w が任意に与えられたとする．この時，係数が 0 でない項の添数は $\mathcal{D}$ の元 D の点と一致する．D の 3 点 i, j, k をとり v_i, v_j, v_k における w の係数が同符号をもつ様にできる．$\{i, j, k\}$ に D の外の元を加えて 4 点集合 S をつくり，対応する $\cdot 0$ の元 ξ_S をとる．この時 D は S による 6×4 分割に$(3, 1^5)$の形に分配される．したがって $\xi_S(w)$ は $(-3, 1^{23})$ 型の元である．

さて群 N は明らかに $(-3, 1^{23})$ 型の元全体がつくる集合に可移に作用している．M の元により ± 3 は v_∞ の係数となるように移せるし，符号は ε_T により全部正にすることができるからである．したがって Λ_2 の任意の元は $\cdot 0$ の元によって $v_\Omega - 4v_\infty$ に移せるから $\cdot 0$ は Λ_2 上に可移に作用している．

Λ_3 の場合も同様である．まず次の補題を証明しよう．$S \in \mathcal{C}_{12}$ の中に 2 点 a, b が与えられた時，適当に $D \in \mathcal{D}$ をとれば $S \cap D = \{a, b\}$ となる．S の中に a, b を含む 5 点集合をとれば，それを含む $\mathcal{D}$ の元 D' が一意的に定まる．ところで (4.7) により $S \cap D'$ は偶数個の点を含む．しかし $D' \subset S$ とはならない．もし $D' \subset S$ ならば $S + D'$ は 4 点集合となり (4.9) に矛盾するからである．したがって $S \cap D'$ は 6 点集合で a, b および 4 点集合 T からなり立つ．そこで T による 6×4 分割 $\{T_i\}$ を考えれば，S の元は $(4, 2, 2, 2, 2, 0)$ と分配される．(S は $\mathcal{D}$ の元を含まない．) しかも $\{a, b\}$ を含む T_i がある．S の元を含まない T_j があるから $D = T_i \cup T_j$ とおけば (4.13) により D は $\mathcal{D}$ の元であって $S \cap D = \{a, b\}$ をみたしている．

さて (2^{12}) 型の元では -2 の数は偶数である．その制限の下で各項の符号は任意に変えることができる（上の補題により任意の 2 元の符号を変える E の元がある)．したがって任意に (2^{12}) 型の元が与えられれば，符号を適当に変え，その上で 4 点集合を適当に選び，対応する 6×4 分割に ± 2 が $(4, 2^4)$ の形に分配され，しかも 4 点集合 T の上で符号も込めて$(2, 2, 2, -2)$となるようにできる．そこで ξ_T による像をとれば $(2, 2, 2, -2) \to (0, 0, 0, \pm 4)$，すなわち$(2^{12})$型の元は$(4, 2^8)$型の元に移される．

任意に $(4, 2^8)$ 型の元が与えられれば，± 4 の符号を適当に変えた上で 4 点集合 T を適当に選んで，T の上で $(\pm 4, \pm 2, \pm 2, \pm 2)$ となり符号は皆同じにすることができる．この時 P により $(4, 2, 2, 2) \to (-1, -3, -3, -3)$ だから

$(4,2^8)$ 型の元は $(-3^3,1^{21})$ 型の元に移る．また $(-3,-3,-3,1)\to(1,1,1,5)$ だから任意の $(-3^3,1^{21})$ 型の元を $(5,1^{23})$ 型の元に移す $\cdot 0$ の元がある．明らかに N の元により任意に選んだ $(5,1^{23})$ 型の元は $v_\Omega+4v_\infty$ に移すことができるから $\cdot 0$ は Λ_3 の上に可移に作用する．

Λ_4 の場合も同様である．$(4^2,2^8)$ 型，$(4,2^{12})$ 型では符号を（それぞれの場合の制限の下で）自由に変えられる．(2^{16}) 型の場合，符号を自由に変えるわけには行かないが (2^{16}) 型の元が与えられれば，それを $(4,2^{12})$ 型，または $(4^2,2^8)$ 型または (4^4) 型の元に移す $\cdot 0$ の元がある．Λ_3 の場合と同様に，Λ_4 の任意の元は $\cdot 0$ の元により $(5,-3^2,1^{21})$ 型の元に移されることが証明される．明らかに N は $(5,-3^2,1^{21})$ 型の元の上に可移に作用するから $\cdot 0$ は Λ_4 上可移である．

ところで $8v_\infty\in\Lambda_4$ であって，$8v_\infty$ の安定化群は N に含まれる(4.24)．そこでこの安定化群を K とおけば，$\cdot 0$ が Λ_4 上可移だから

$$|\cdot 0:K|=|\Lambda_4|$$

を得る．明らかに $8v_\infty$ は N の元により $\pm 8v_i$ に移るから $|N:K|=48$．これから N の指数と $\cdot 0$ の位数が定理にあげた値となることが証明される．▯

注意 Conway 群 $\cdot 0$ は Λ_2 上可移だから Λ_2 の 1 点の安定化群の指数は $|\Lambda_2|$ に等しい．よって上定理および (4.18) から $\cdot 2$ の位数が計算される．Conway 群 $\cdot 3$ の場合も同様である．▯

3. Conway 群の単純性　M の元 α は前に定義した通りとする $(\alpha(x)=x+1)$．ここで $A=\langle\alpha\rangle$, $G=\cdot 0$ とおき次の補題の成り立つことを証明しよう．

(4.27) Conway 群 $\cdot 0$ の中で元 α の中心化群は $\langle -1\rangle\times A$ である．

証明 α の定義から明らかなように，α を表現する行列の固有値は 1 の 23 乗根である．そのうち 1 の重複度は 2，その他の根の重複度は 1 である．したがって α による不変ベクトルの全体は 2 次元の部分空間をつくり，その基として

$$v=v_\infty,\quad w=\textstyle\sum_{i\neq\infty}v_i$$

をとることができる．いま $\sigma\in C_G(\alpha)$ とすれば σ は α の不変元を α の不変元に移すから $\sigma(v)=av+bw$ となる．ここで定理 4.21 により $n=8a$ および $m=8b$ は共に整数である．v の長さが 1 だから $a^2+23b^2=1$ を得る．よって

$n^2+23m^2=64$. ところで n, m は整数だから $m=0$ を得る. すなわち $\sigma(v)=\pm v$ が成り立つ. よって (4.24) により $\sigma\in N$ を得る. N は E と M との半直積だから

$$C_G(\alpha)=C_N(\alpha)=C_E(\alpha)C_M(\alpha)$$

が成り立つ. α 不変な $\mathscr{C}$ の元は空集合と Ω だけであるから $C_E(\alpha)=\langle -1\rangle$ となる. α は 23 巡回置換だから $C_M(\alpha)=A$, すなわち(4.27)が成り立つ. ▯

定理 4.28 Conway 群 ·0 の中心は $\langle -1\rangle$ と一致する.

証明 中心は α の中心化群に含まれるから明らかに定理が成り立つ. ▯

Conway 群の位数から A が G のシロー群の一つであることがわかる. そこで

$$A\subset C_G(A)\subset N_G(A)\subset G$$

において指数 $|G:N_G(A)|$ は 23 を法として 1 に合同である(シローの定理). また $C_G(A)\lhd N_G(A)$ で $N_G(A)/C_G(A)$ は A の自己同形群の部分群である. この場合 Aut A は位数 22 の巡回群である(『群論』上 p. 46(6.10)). さて

$$|G:C_G(A)|=2^{21}3^9 5^4 7^2 11\cdot 13$$

(定理 4.26 および (4.27)) だから $|G:C_G(A)|\equiv 11 \pmod{23}$. これから次の補題が証明される.

(4.29) $|N_G(A):C_G(A)|=11$, 特に $N_G(A)\subset\langle -1\rangle\times M$ が成り立つ.

証明 シローの定理により $|G:N_G(A)|\equiv 1 \pmod{23}$ だから

$$|N_G(A):C_G(A)|\equiv 11 \pmod{23}.$$

一方, この左辺は高々 22 だから前半が成り立つ. 位数を考え合わせれば -1, α, β が $N_G(A)$ を生成することがわかる. よって後半も成り立つ. ▯

Conway 群の単純性を証明するために次の定理が用いられる.

(4.30) 一般に群 G の正規部分群を H とし H のシロー群を P とする.

(i) $G=HN_G(P)$.

(ii) G の位数の素因数 p は $|H|$ または $|N_G(P)|$ の約数である.

証明 任意の元 $x\in G$ に対し xPx^{-1} は H のシロー群である. したがってシローの定理により $xPx^{-1}=yPy^{-1}$ をみたす H の元 y がある. よって

$$y^{-1}xPx^{-1}y=y^{-1}xP(y^{-1}x)^{-1}=P,$$

すなわち $y^{-1}x\in N_G(P)$ を得る. これから $x\in HN_G(P)$ となり (i) が成り立

つ．同形定理により $|G:H|=|HN_G(P):H|=|N_G(P):N_G(P)\cap H|$ を得る．したがって素因数 p は $|H|$ または $|N_G(P)|$ の約数となる．□

定理 4.31　Conway 群 ·0 において，-1 を含む正規部分群は $\langle -1\rangle$ および ·0 だけである．中心による商群 ·1 は単純である．

証明　Conway 群 ·0 の中心 $\langle -1\rangle$ を含む正規部分群を H とする．

まず $|H|$ が 23 で割れる場合を考えよう．この時 H は位数 23 の部分群を含んでいる．それは A と共役だから $A\subset H$. そこで (4.30) により

$$G=HN_G(A)$$

を得る．ところで $A\subset M=M_{24}$ で M は単純だから，M は A の共役群全体で生成される．A と共に A の共役群は H に含まれているから $M\subset H$ となる．仮定により $-1\in H$ だから $\langle -1\rangle\times M\subset H$, よって $N_G(A)\subset\langle -1\rangle\times M$ は H の部分群である．すなわち $G=HN_G(A)=H$ が成り立つ．

次に $|H|$ が 23 で割れない場合を考えよう．H の任意のシロー群を P とする．(4.30)により $N_G(P)$ の位数は 23 で割り切れる．したがって $N_G(P)$ は位数 23 の元 σ を含んでいる．元 σ は A の元と共役だから (4.27) により σ の中心化群の位数は 46 である．さて P の位数が奇数であるとすれば σ は P の非単位元と可換ではない．したがって σ の作用による $P-\{1\}$ の軌道の大きさはすべて 23, よって $|P|\equiv 1 \pmod{23}$ となる．しかし G の位数をみればこれは不可能である．すなわち H の位数は 2 のベキである．この場合

$$|H|\equiv 2 \pmod{23}$$

が成り立つ．よって $|H|=2$ または $|H|=2^{12}$ である．位数 2^{12} の正規部分群が存在したと仮定しよう．$C_G(H)\lhd G$ であるが $C_G(H)$ は G と一致しない（α は $C_G(H)$ の元ではない）．したがって既に証明したように $C_G(H)$ は 2 群である．ところで G は位数 13 の元 ρ を含んでいる．この元 ρ の不変元のつくる部分群の位数を 2^a とすれば $a\geqq 1$ かつ $2^{12}\equiv 2^a \pmod{13}$ が成り立つ．これから $a=12$ を得る．これは $\rho\in C_G(H)$ と同値であるから既に証明したことに矛盾する．したがって位数 2^{12} の正規部分群は存在しない．$|H|=2$ ならば $H=\langle -1\rangle$ で H は中心に一致する．同形対応定理により中心による商群 ·1 は単純群であることが証明される．□

定理 4.32　Conway 群 ·2 および ·3 は共に単純群である．

証明 Conway 群 $\cdot 0$ は Λ_2 上可移だから $\cdot 2$ を定義するために Λ_2 のどの元の安定化群を考えても同形の群が得られる．$(-3, 1^{23})$ 型の元を用いれば $\cdot 2$ が M_{23} を含んでいることがわかる．ここで $\langle\alpha, \beta\rangle\subset M_{23}$ であることを注意しておく．定義により $\cdot 2$ は元 -1 を含んでいない．よって $N_G(A)\subset M_{23}$.

さて H を $\cdot 2$ の正規部分群とする．$|H|$ が 23 で割れる場合には前と同様に $\alpha\in H$ を得る．ところで $\alpha\in M_{23}$ で M_{23} は単純だから定理 4.31 の証明と同様に（M_{24} の代りに M_{23} を用いて）$H=\cdot 2$ が証明される．

H の位数が 23 で割れない場合には前と同様に H が 2 群であることが証明される．そこで $H\neq\{1\}$ と仮定すれば $|H|=2^{11}$ となる．また $C_G(H)\neq 1$ より

$$C_G(H)=H$$

が成り立つ．したがって H は位数 2^{11} の基本可換群である．そこで $\cdot 2=G$ とおけば G/H は Aut H の部分群に同形である(『群論』上 p. 47)．ところで H が位数 2^{11} の基本可換群であるから Aut H は $SL(11, 2)$ に同形である．$|G/H|$ の位数は 5^3 で割れるが $SL(11, 2)$ の位数は 5^3 では割り切れない．これは矛盾であるから位数 2^{11} の正規部分群は存在しない．よって $\cdot 2$ は単純である．

Conway 群 $\cdot 3$ の場合も同様である．$\cdot 3$ を定義するのに $(5, 1^{23})$ 型の元を用いれば $\cdot 3$ は M_{23} を含んでいることがわかる．よって前と同様に位数が 23 で割り切れる正規部分群は $\cdot 3$ と一致する．位数が 23 で割り切れない場合にはどのシロー群 P をとっても $|P|\not\equiv 1 \pmod{23}$ となる（$\cdot 3$ の位数は 2^{11} で割れない）．したがってこの場合 $H=\{1\}$ となり $\cdot 3$ も単純群となる．□

文　　献

本書で必要となる代数の諸定理および群論からの予備定理は

秋月・鈴木，代数 I，II，岩波書店

鈴木，群論，上・下，岩波書店

から引用した．これらの本はそれぞれ『代数』I，『群論』上，などと引用されている．

その外，次の本に関連した事項がのっている．

[1] N. Bourbaki, Groupes et algèbres de Lie Chap. 4,5 et 6, Hermann, Paris, 1968.

[2] R. Carter, Simple groups of Lie type, Wiley-Interscience, New York, 1972.

[3] 松島与三，リー環論，共立出版．

[4] 永尾　汎，群とデザイン，岩波書店．

[5] 大山　豪，有限置換群，裳華房．

[6] R. Steinberg, Lectures on Chevalley groups, Lecture notes, Yale University, 1968.

[7] R. Steinberg, Endomorphisms of Linear Algebraic Groups, Memoirs AMS **80**, 1968.

[8] J.-P. Serre, Algèbres de Lie semi-simples complexes, W. A. Benjamin, New York, 1966.

本書で引用した論文のうち番号に＊印のついているものについては『群論』上の巻末にある文献表の対応する番号を参照のこと．散在群 F_1 については次にあげる Griess[3] を参照されたい．

[1] M. Aschbacher, Finite groups generated by odd transposition I—IV, Math. Z. **127**(1972) 44—56, J. of Algebra **26**(1973) 451—491.

[2] B. Fischer, D. Livingstone, M. Thorne, The character table of the monster (未発表．Atlas 参照)．

[3] R. L. Griess, The friendly giant, Invent. Math. **69**(1982), 1—102.

[4] D. Livingstone, On a permutation representation of the Janko group, J. of Algebra **6**(1967) 43—55.

[5] J. Tits, Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples, Publ. Math., Inst. Hautes Etudes Sci. **31**(1966) 21—58.

索　　引

著　者

鈴　木　通　夫

1926年千葉市に生まれる．1948年東京大学理学部数学科卒業．1952年東京教育大学助教授，1958年イリノイ大学教授，1968年同大学 Center for Advanced Study 教授併任，現在に至る．理学博士．1974年度日本学士院賞受賞．

著書：Structure of a group and the structure of its lattice of subgroups (Springer-Verlag)，群論上下（岩波書店），代数 I, II（秋月康夫と共著，岩波書店）．

有　限　単　純　群

定価 7000 円

1987年10月28日　第1刷発行

発行所　株式会社　紀伊國屋書店
東京都新宿区新宿3の17の7
電　話 03 (354) 0131 (代表)
振替口座　東京 9-125575

出版部　東京都世田谷区桜丘5の38の1
電　話 03 (439) 0125 (代表)
郵便番号 156

ISBN 4-314-00490-8 C3341
PRINTED IN JAPAN

印 株　研究社印刷
製 本　三　水　舎

紀伊國屋数学叢書について

数学を学ぶにはいろいろの段階があるが，いずれの場合でも書物などによって自学自習することが最も重要であり，単に講義を聞くというような受動的な勉強だけでは，はなはだ不十分である．

みずから学ぶために現在いろいろな数学書が出版されている．しかし，数学の進歩は極めて基礎的な考え方に対してさえ常に影響を与えており，従ってどのような段階の勉強であっても，常に新しい考え方を理解することが必要である．このためには，数学の過去と将来とを結ぶ視点から書かれた書物が数多く出版されることが望ましい．即ち，新しい視点と古典的な視点とを見くらべ，基本的なことをも将来の発展を考慮した視点から説明するという立場で書かれた書物が要望されている．

本叢書はこのような要望に応えて企画されたものであって，各巻が大学理工学系の専門課程の学生または大学院学生がそれぞれの分野での話題，対象について入門の段階からある程度の深さまで勉学するための伴侶となることを目指している．このために我々は各巻の話題の選択について，十分配慮し，現代数学の発展にとって重要であり，また既刊書で必ずしも重点が置かれていないものを選び，各分野の第一線で活躍しておられる数学者に執筆をお願いしている．

学生諸君および数学同好の方々が，この叢書によって数学の種々の分野における基本的な考え方を理解し，また基礎的な知識を会得することを期待するとともに，更に現代数学の最先端へ向かおうとする場合の基礎ともなることを望みたい．